腾讯安全

# 《2020年公有云安全报告》

腾讯安全

2021年2月

# 一、报告背景

产业互联网时代，云计算 IT 架构以更简单的架构设计、更高的性价比、更灵活的系统颠覆了传统 IT 基础架构，但随着算力、IT 架构、攻防节奏、以及数据资产的不断变化，也为云上安全提出了新的挑战。

随着业务上云的兴起，安全攻防的主战场也转而上云。在腾讯全球数字生态大会上，腾讯副总裁丁珂指出，“产业互联网让国民经济更具韧性，也让有准备的企业家迎来新的机遇。产业上云，安全先行，在数字化升级过程中，要以战略视角、产业视角和生态视角去看待安全，进行前置部署。“

对于多数处于数字化转型期的企业来说，安全设备、研发投入、人才招聘的成本负担很高，从零开始自建防御体系难度颇大，企业上云是应对数字时代安全问题的“最优解”。

腾讯在网络安全耕耘 20 余年的经验，拥有 7 大安全实验室超过 3500 人的专业安全团队。依托云原生安全思路，我们构建了云适配的原生安全产品架构，既可以有效地保障腾讯云平台自身安全，也能让云上企业有效降低安全运营门槛、提升整体的安全水位。使得公有云的政企用户在面临来自世界各地的网络攻击时，仍能从容应对。

本报告将 2020 年，针对公有云的攻击特点进行总结，帮助政企用户更全面的掌控云上安全风险，及时采用正确的应对措施，化解网络安全威胁，让 IT 平台更好地服务业务和最终用户。

# 二、云上安全风险

## 1、恶意木马

### 1.1 恶意木马趋势

云上恶意木马事件在下半年有明显上升。


图 1

从恶意木马检出结果来看，有 6.3%的公司曾在一个月内发现恶意木马事件，这一数据表明云上主机发生恶意木马入侵事件已不是小概率事件（统计学上，通常将概率低于 5%称为小概率事件。）

### 1.2 恶意木马类型 Top 榜

从检出的恶意木马统计可以发现，公有云用户所中木马的类型主要为感染型木马、DDoS 攻击木马和后门木马。感染型木马具有主动扩散能力，建议发现主机存在感染型木马

时，立即进行全盘扫描，防止进一步扩散。

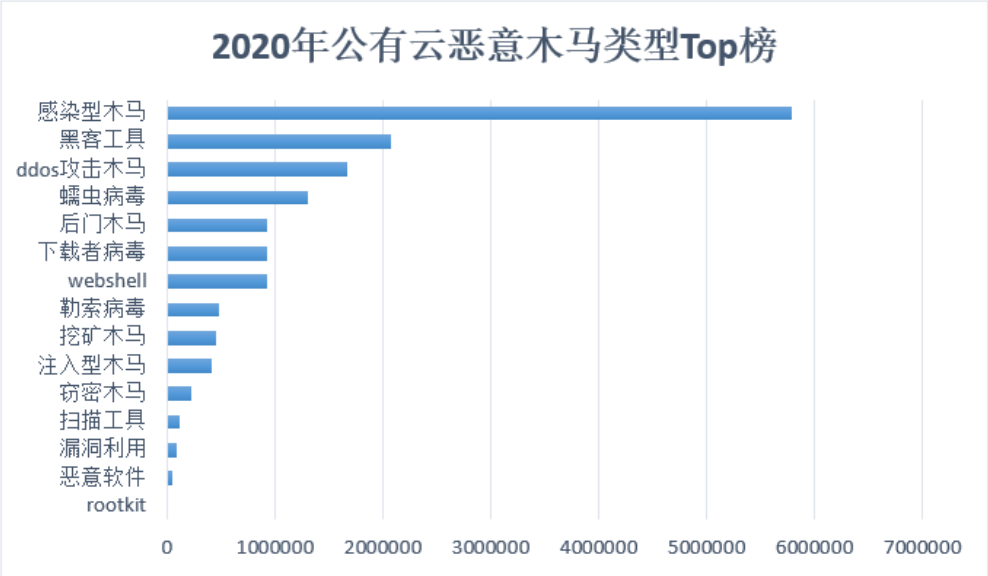


图 2

## 1.3 恶意木马处理情况

在发现的恶意木马中，有 27%的恶意木马未及时处理，建议及时处理，防止进一步扩散。此外有 1%的病毒木马被信任，这是个值得警惕的指标，强烈建议不要轻易将恶意木马添加至信任区。

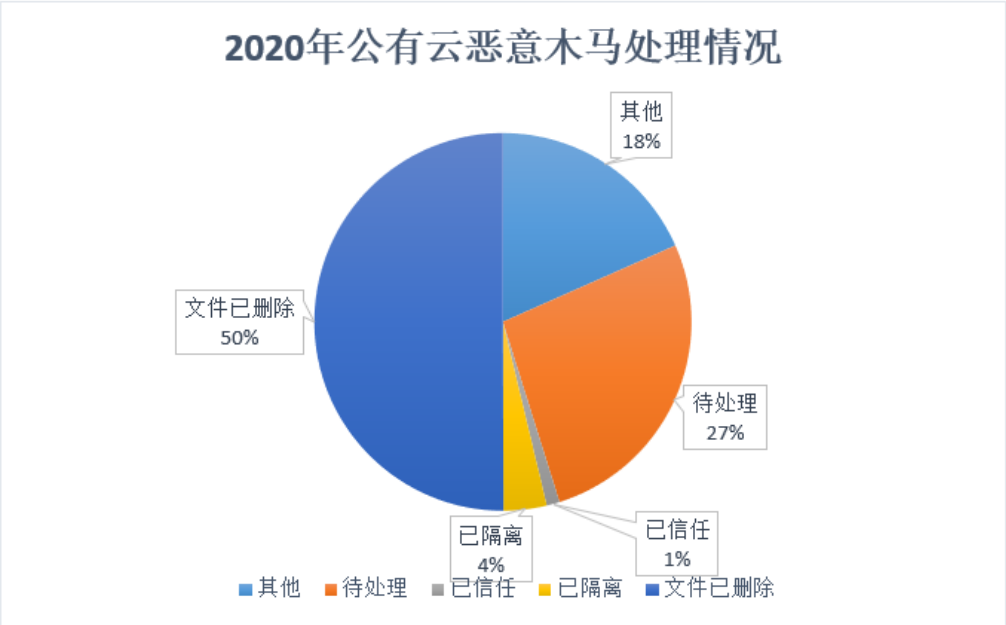


图 3

## 1.4 典型案例

### Mirai 僵尸网络利用 Apache Hadoop Yarn 资源管理系统 REST API 未授权访问漏洞入侵云主机

腾讯安全威胁情报中心检测到 Mirai 僵尸网络利用 Apache Hadoop Yarn 资源管理系统 REST API 未授权访问漏洞入侵云主机，入侵传播的 Mirai 木马会通过 C&C 服务器下发命令进行 DDoS 攻击。

早在 2018 年腾讯云鼎实验室就披露过恶意软件利用 Hadoop Yarn REST API 未授权漏洞入侵挖矿的案例（https://www.freebuf.com/vuls/173638.html）。两周前，腾讯安全威胁情报中心发现“永恒之蓝”下载器木马最新变种同样利用该漏洞进行攻击传播（https://mp.weixin.qq.com/s/953ZHaf8IjLGyxB3tWSoDQ）。可见，由于运维人员在创建容器集群时缺乏安全意识，未对 Hadoop Yarn 进行安全配置，致使越来越多的黑客通过该漏洞入侵云服务器。

参考链接：https://mp.weixin.qq.com/s/IdKj2OZmVIUcj9RSERdlTQ

### 挖矿木马团伙 z0Miner 利用 Weblogic 未授权命令执行漏洞（CVE-2020-14882/14883）的攻击行动

腾讯主机安全（云镜）于 2020.11.02 日捕获到挖矿木马团伙 z0Miner 利用 Weblogic 未授权命令执行漏洞（CVE-2020-14882/14883）的攻击行动。该团伙通过批量扫描云服务器发现具有 Weblogic 漏洞的机器，发送精心构造的数据包进行攻击。之后执行远程命令下载 shell 脚本 z0.txt 运行，再利用该 shell 脚本植入门罗币挖矿木马、挖矿任务本地持久化，以及通过爆破 SSH 横向移动。根据该团伙控制的算力推算，已有大约 5000 台服务器

受害。

由于 Weblogic 未授权命令执行漏洞（CVE-2020-14882/14883）10 月 21 日才被官方公布，有许多企业未来得及修复，同时该漏洞的补丁存在被绕过的风险。因此该挖矿木马可能对云主机造成较大威胁。

参考链接：https://mp.weixin.qq.com/s/cyPZpB4zkSQccViM0292Zg

## 腾讯主机安全（云镜）捕获 Kaiji DDoS 木马通过 SSH 爆破入侵

腾讯安全威胁情报中心在为客户提供安全巡检服务时，发现腾讯主机安全（云镜）告警 SSH 爆破入侵事件，遂对事件进行溯源追查，溯源到有疑似国内黑客开发的木马 Kaiji 通过 22 端口弱口令爆破入侵服务器。攻击者入侵云主机会下载二进制木马将自身安装到系统启动项进行持久化，并且可根据 C2 服务器返回的指令进行 DDoS 攻击。

参考链接：https://mp.weixin.qq.com/s/hacyPAA82rgEBivwOYhuEg

## Mykings 僵尸网络新变种传播 PcShare 远程控制木马

腾讯安全威胁情报中心检测到 Mykings 挖矿僵尸网络变种木马，更新后的 Mykings 会在被感染系统安装开源远程控制木马 PcShare，对受害电脑进行远程控制：可进行操作文件、服务、注册表、进程、窗口等多种资源，并且可以下载和执行指定的程序。

Mykings 僵尸网络木马还会关闭 Windows Defender、检测卸载常见杀毒软件；卸载竞品挖矿木马和旧版挖矿木马；下载“暗云”木马感染硬盘主引导记录（MBR)实现长期驻留；通过计划任务、添加启动项等实现开机自动运行等行为。

MyKings 僵尸网络最早于 2017 年 2 月左右开始出现，该僵尸网络通过扫描互联网上 1433 及其他多个端口渗透进入受害者主机，然后传播包括 DDoS、Proxy (代理服务)、RAT

（远程控制木马）、Miner（挖矿木马）、暗云 III 在内的多种不同用途的恶意代码。由于 MyKings 僵尸网络主动扩散的能力较强，影响范围较广，对企业用户危害严重。根据门罗币钱包算力 1000KH/s 进行推测，Mykings 僵尸网络目前已控制超过 5 万台电脑进行挖矿作业。

参考链接：https://mp.weixin.qq.com/s/wZvnq6gVnEdGSH6f6oG8MA

## Muhstik 僵尸网络通过 SSH 爆破攻击国内云服务器

腾讯安全威胁情报中心检测到大量源自境外 IP 及部分国内 IP 针对国内云服务器租户的攻击。攻击者通过 SSH（22 端口）爆破登陆服务器，然后执行恶意命令下载 Muhstik 僵尸网络木马。该僵尸网络会控制失陷服务器执行 SSH 横向移动、下载门罗币挖矿木马和接受远程指令发起 DDoS 攻击。

腾讯安全威胁情报中心经过用户授权，对此次攻击进行溯源分析，发现国内多家知名企业的云服务器均受到该僵尸网络攻击，目前已有上千台服务器沦陷受害。腾讯安全专家建议相关企业采取必要措施，拦截入侵者，恢复已失陷的系统。

参考链接：https://mp.weixin.qq.com/s/ExBUifhDQTQEbU3sz7WNVA

## GuardMiner 挖矿木马活跃，具备蠕虫化主动攻击能力

腾讯安全威胁情报中心检测到跨平台挖矿木马 GuardMiner 近期十分活跃，该木马会扫描攻击 Redis、Drupal、Hadoop、Spring、thinkphp、WebLogic、SQLServer、Elasticsearch 多个服务器组件漏洞，并在攻陷的 Windows 和 Linux 系统中分别执行恶意脚本 init.ps1，init.sh，恶意脚本会进一步下载门罗币挖矿木马、清除竞品挖矿木马并进行本地持久化运行。在 Linux 系统上利用 SSH 连接和 Redis 弱口令爆破进行内网扩散攻击。

因挖矿守护进程使用文件名为 sysguard、sysguerd、phpguard，腾讯安全威胁情报中心将该挖矿木马命名为 GuardMiner。

因该病毒已具备蠕虫化主动攻击扩散的能力，近期已有较多企业中招。腾讯安全专家建议政企机构尽快修复服务器组件漏洞，相关服务避免使用弱口令。腾讯安全系列产品均可检测并协助清除 GuardMiner 挖矿木马。

参考链接：https://mp.weixin.qq.com/s/-nUrNilr-iq7kbmopaqXwA

## 2、云上勒索

一部分黑客入侵云主机之后，会尝试实施勒索攻击，腾讯安全目前观察到针对云上勒索的攻击有两类情况：数据库锁库勒索和勒索病毒加密。幸运的是，大量黑灰产业攻击云上主机，最终用来挖矿的最为常见，其次是作为攻击跳板或控制失陷主机组建僵尸网络，直接实施勒索攻击的相对少见。

一类是数据库锁库勒索，以 mysql 数据库勒索最为常见。攻击过程通常包括 3 步：

1）信息收集：通过开源代码泄露，默认端口扫描等方式，获取到存在 mysql 服务的 IP 列表。

2）爆破攻击：利用密码字典爆破 mysql 密码（一般是扫描 root 账号，使用 NMAP，xHydra，Metasploit 等工具爆破）

3）锁库勒索：利用获取到的 mysql 密码，登录后删除数据库数据勒索。或者直接在数据库内，将原有数据加密后存入新表中（利用 Mysql 自带的 aes 加密函数），然后创建表存储勒索赎金相关信息。

另一类为入侵后下载运行勒索病毒，主要针对 Windows 系统云主机。攻击过程通常为 4 步：

1）信息收集：批量扫描，获取 IP 列表

2）爆破攻击：RDP 爆破

3）登录投毒：登录受害者服务器，横向渗透，或作为跳板对外攻击

4）加密勒索：失去利用价值后，加密本地文件勒索

同样是勒索攻击，黑灰产业针对云上资产的勒索，其危害远不如针对企业私有网络的攻击，对受害者造成的实质性威胁也较小。这其中有个非常重要的原因：政企机构将业务上云之后，较多情况下会部署相对完善的备份、容灾方案。当攻击者发现针对云上主机的勒索攻击屡屡不能得手的时候，云上勒索攻击便无法成为云上威胁的主流。

尽管如此，腾讯安全团队建议业务上云的政企机构切莫小视勒索威胁，攻击者入侵控制云上主机，就有利用被控肉鸡系统牟利的各种可能性，任何时候都不可忽视业务容灾备份的重要性。

# 3、异常登录行为

异常登录为发现非常用登录源、登录地点、用户名等登录了主机，运维人员可将可信的登录源添加至白名单。

## 3.1 异常登录趋势

随着企业上云业务的不断增长，腾讯安全观察到云上主机异常登录事件也呈明显上升趋势，值得企业安全运维人员高度重视。

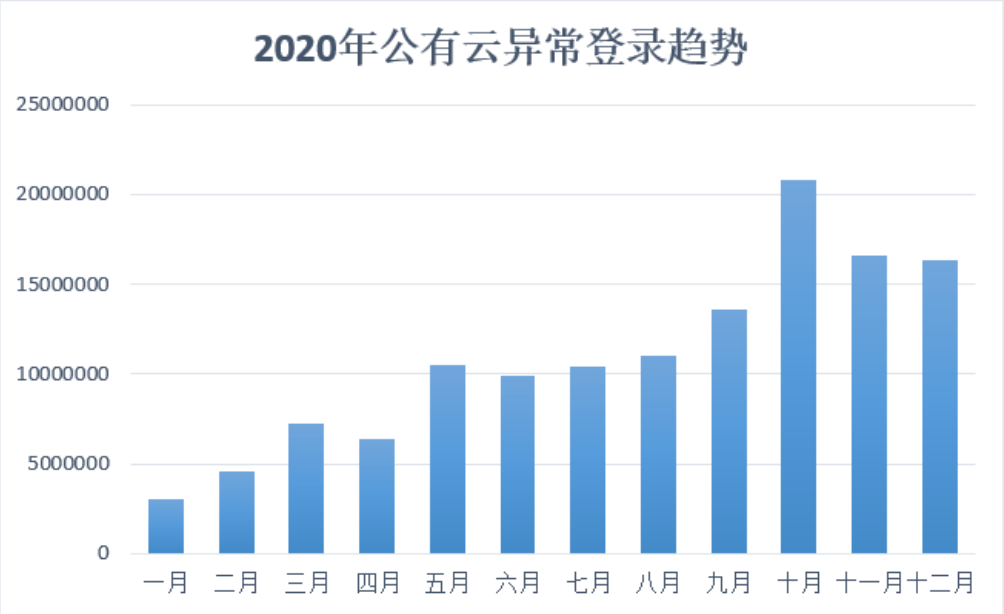


图 4

## 3.2 异常登录端口统计

爆破攻击次数最多的端口为 22，为远程登录服务默认端口，统计数据表明，该端口全年被爆破次数超过 2.5 亿次。

| 端口号 | 异常登录次数 |
|---|---|
| 22 | 258483885 |
| 28 | 15378 |
| 80 | 7629 |
| 64 | 6309 |
| 12 | 5253 |
| 25 | 3687 |
| 44 | 1938 |
| 77 | 1656 |
| 23 | 1524 |
| 67 | 1389 |
| 82 | 1149 |
| 220 | 915 |
| 222 | 915 |
| 122 | 813 |
| 39 | 768 |

图 5

## 3.3 异常登录用户名统计

从 2020 年异常登录情况分析，发现被异常登录次数最多的用户名有 root、work、game、administrator 等常见或默认的用户名。异常登录次数多的达到数千万次，少的有数十万次。

| 用户名 | 异常登录次数 |
| --- | --- |
| root | 64963524 |
| work | 30282303 |
| game | 24677817 |
| administrator | 22908375 |
| L******g | 7273860 |
| ftpuser | 5019234 |
| www | 4514253 |
| Y******n | 4408320 |
| git | 4216050 |
| M******v | 2815611 |
| C*** | 2552460 |
| F*****n | 2206884 |
| zoomeye | 1933380 |
| J*****m | 1587660 |
| upload | 1511376 |

图 6

# 4、服务爆破行为

## 4.1 爆破攻击趋势

爆破攻击在 2020 年有明显上升趋势，最近三个月则有所下降。


图 7

## 4.2 爆破攻击端口统计

爆破次数最多的端口为 22 和 3389，分别是 linux、Windows 远程登录服务默认端口。这两个远程登录服务端口被爆破攻击的次数达到惊人的 32 亿次和 17 亿次。爆破次数最多的端口列表如下：

| 端口号 | 爆破攻击次数 |
|---|---|
| 22 | 3202671399 |
| 3389 | 1784885936 |
| 16888 | 8246212 |
| 17168 | 3099421 |
| 2888 | 3017910 |
| 2222 | 2628970 |
| 62779 | 2441682 |
| 9898 | 1690100 |
| 38666 | 1019226 |
| 22222 | 846659 |
| 28899 | 704414 |
| 33899 | 698086 |
| 58899 | 677351 |
| 2022 | 606894 |

图 8

## 4.3 爆破攻击用户名统计

爆破攻击常用的用户名为 root、admin 和 administrator 等常用默认用户名。下表也显示了安全运维人员大量使用的最常见用户名，爆破攻击次数最少的也超过 4000 万次，linux 系统默认根用户 root 全年被爆破攻击的次数超过 37 亿次，Windows 默认用户名 administrator 则被爆破攻击近 33 亿次。

常用用户名被爆破攻击的次数统计如下：

| 用户名 | 爆破攻击次数 |
|---|---|
| root | 3744730734 |
| administrator | 3290198157 |
| admin | 2153775399 |
| 111111 | 407956308 |
| operator | 280481217 |
| adm | 265923531 |
| ftp | 220078608 |
| 123321 | 208194027 |
| 1234 | 174149067 |
| nobody | 134253243 |
| hp | 117285510 |
| user | 103209717 |
| oracle | 83274492 |
| mysql | 73247424 |
| 123 | 69608994 |
| samurai | 67801074 |
| guest | 58256916 |
| test | 47787912 |

图 9

# 5、漏洞风险

## 5.1 漏洞风险趋势

在 2020 年 12 月，漏洞风险有显著上升，主要是因为 OpenSSL 拒绝服务漏洞(CVE-2020-1971)漏洞的披露。OpenSSL 组件由于应用极其普及，属于互联网基础服务，一旦出现高危漏洞，整个网络风险形势就会巨变，如果漏洞出现不及时修复，企业网络就有极大可能遭遇严重事件。


图 10

有 54%的企业在 3 天内发现过漏洞风险，意味有较多企业服务组件存在安全漏洞风险而没有及时修复。

## 5.2 漏洞风险类型

主要存在的漏洞风险类型统计，前三位分别是拒绝服务漏洞、远程代码执行和任意文件读取漏洞。

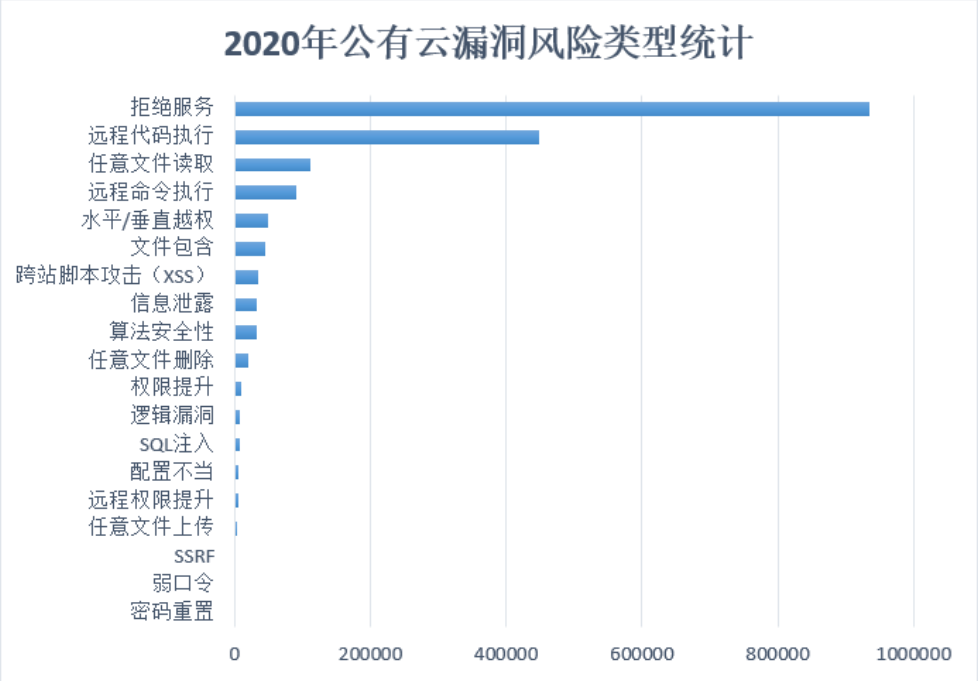


图 11

## 5.3 漏洞风险 Top 榜

主要存在的漏洞风险为 OpenSSL 拒绝服务漏洞(CVE-2020-1971)、Spring 框架反射型文件下载漏洞和 Jackson 远程代码执行漏洞。

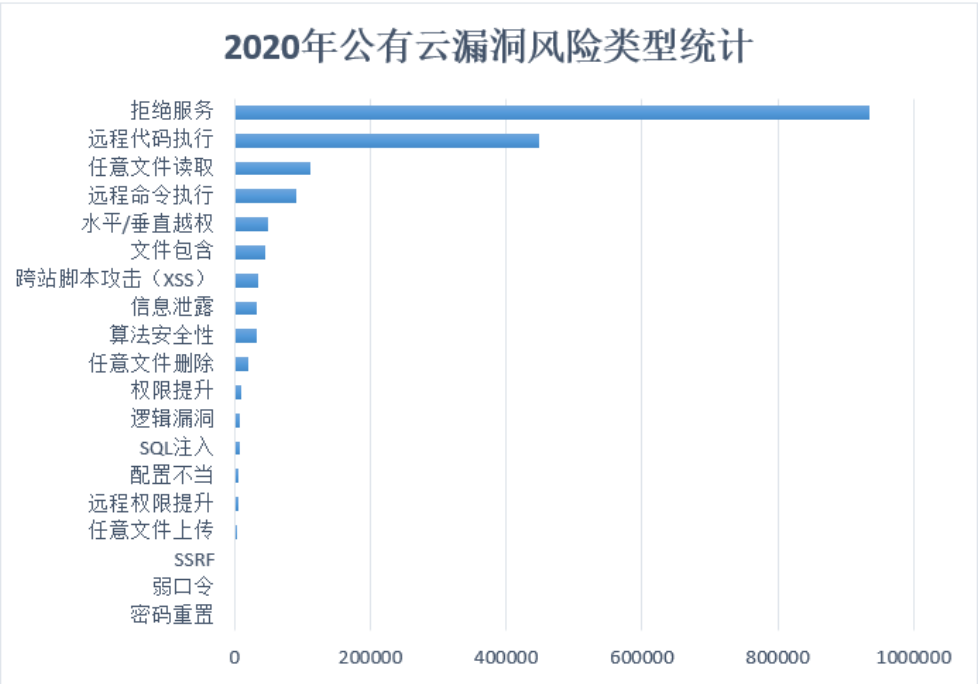


图 12

## 5.4 漏洞风险等级

根据漏洞风险等级统计，高危占 45%，中危 54%，严重及低危漏洞占比较少，合计仅 1%。

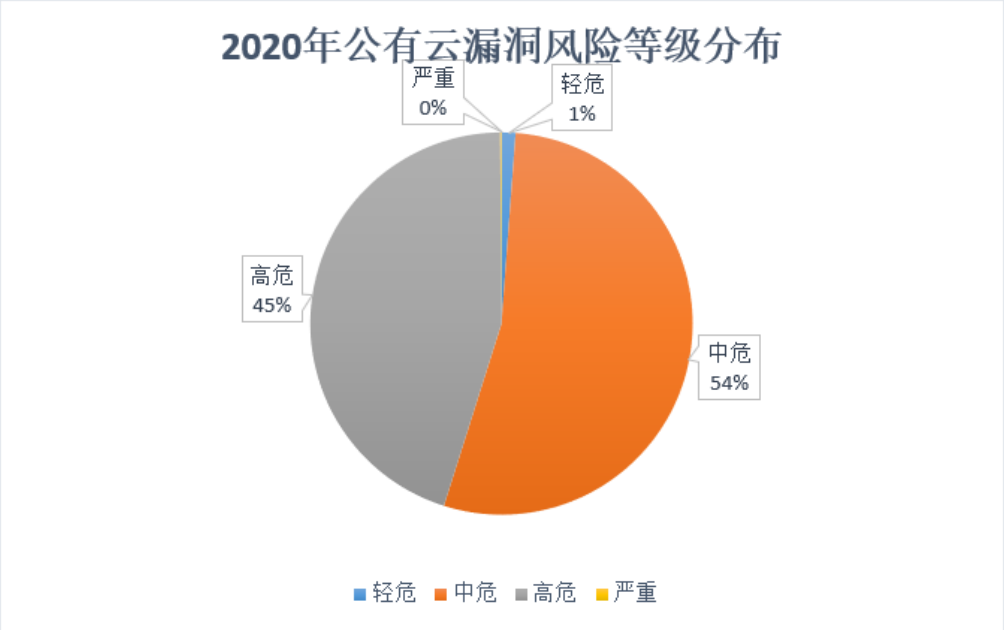


图 13

## 5.5 漏洞利用典型案例

### 4SHMiner 利用 Apache Shiro 反序列化漏洞 CVE-2016-4437 针对云服务器的攻击

腾讯主机安全(云镜)捕获到挖矿木马 4SHMiner 利 Apache Shiro 反序列化漏洞 CVE-2016-4437 针对云服务器的攻击行动。4SHMiner 挖矿团伙入侵成功后会执行命令下载 4.sh，然后下载 XMRig 挖矿木马并通过 Linux service、systemctl 服务，系统配置文件 $HOME/.profile，crontab 定时任务等实现持久化运行。

通过其使用的门罗币钱包算力(约 333KH/s)进行推算，4SHMiner 挖矿木马团伙已控制约 1.5 万台服务器进行挖矿，根据算力突变数据可知其在 2020.11.16 至 17 日一天之内就

新增感染近 1 万台机器。腾讯安全专家建议企业及时检查服务器是否部署了低于 1.2.5 版本的 Apache Shiro，并将其升级到 1.2.5 及以上版本。

参考链接：https://mp.weixin.qq.com/s/iwtcUsiAOpOtDm79lsOXWw

## 永恒之蓝下载器木马新增利用 Hadoop Yarn 未授权访问漏洞攻击

腾讯安全威胁情报中心检测到永恒之蓝下载器木马新增利用 Hadoop Yarn 未授权访问漏洞攻击。该变种入侵 Linux 服务器后下载门罗币挖矿木马，然后将挖矿任务进行持久化、清除竞品挖矿木马，并通过 SSH 爆破横向移动。

永恒之蓝下载器木马自 2018 年底出现以来，一直处于活跃状态。该病毒不断变化和更新攻击手法，从最初只针对 Windows 系统扩大攻击范围到 Linux 系统。截止目前，其攻击手法已涵盖弱口令爆破、系统漏洞利用、Web 漏洞利用等，其中利用 SSH、Redis、Hadoop Yarn 服务的攻击方式可能对云主机以及云上业务造成较大威胁。

参考链接：https://mp.weixin.qq.com/s/953ZHaf8IjLGyxB3tWSoDQ

## BuleHero 挖矿蠕虫利用 Apache Solr 远程代码执行漏洞(CVE-2019-0193)进行攻击

腾讯安全威胁情报中心研究人员在日常巡检中发现，有攻击者利用 Apache Solr 远程代码执行漏洞（CVE-2019-0193）对某客户进行攻击，由于客户部署的腾讯云防火墙已对该类型攻击进行识别并设置为“阻断”，该攻击事件未对客户 IT 资产造成影响。

腾讯安全专家对该事件进一步分析后发现，此次攻击属于 BuleHero 挖矿蠕虫病毒，且该变种版本新增了 SMBGhost（CVE-2020-0796）漏洞利用代码。

该团伙擅长利用各类 Web 服务器组件漏洞进行攻击，包括：Tomcat 任意文件上传漏

洞、Apache Struts2 远程代码执行漏洞、Weblogic 反序列化漏洞、Drupal 远程代码执行漏洞、Apache Solr 远程命令执行漏洞、PHPStudy 后门利用均在其武器列表中。此外还会利用永恒之蓝漏洞、$IPC 和 MSSQL 弱口令爆破等等攻击手法，攻击成功后，会在目标机器植入门罗币挖矿木马和远控木马。

参考链接：https://mp.weixin.qq.com/s/3dfWy7EGfGRMgES0Z8xlpg

# 6、安全基线风险

安全基线，是明确企业网络环境中相关设备与系统达到最基本的防护能力而制定的一系列安全配置基准，腾讯主机安全（云镜）内置国际标准基线、等保二级、等保三级、弱密码、未授权访问、腾讯安全标准等基线标准。通过安全基线检测，指导企业基于安全基线管理网络资产，使网络信息系统达到等保合规要求，能够最大限度减少被黑客攻击入侵的可能性。

## 6.1 安全基线问题趋势

从检测结果看，随着企业上云的主机越来越多，检出存在安全基线风险的主机数量也有上升趋势。需要企业安全运维人员更加重视基线检测结果，使企业网络运营环境符合基准安全要求。

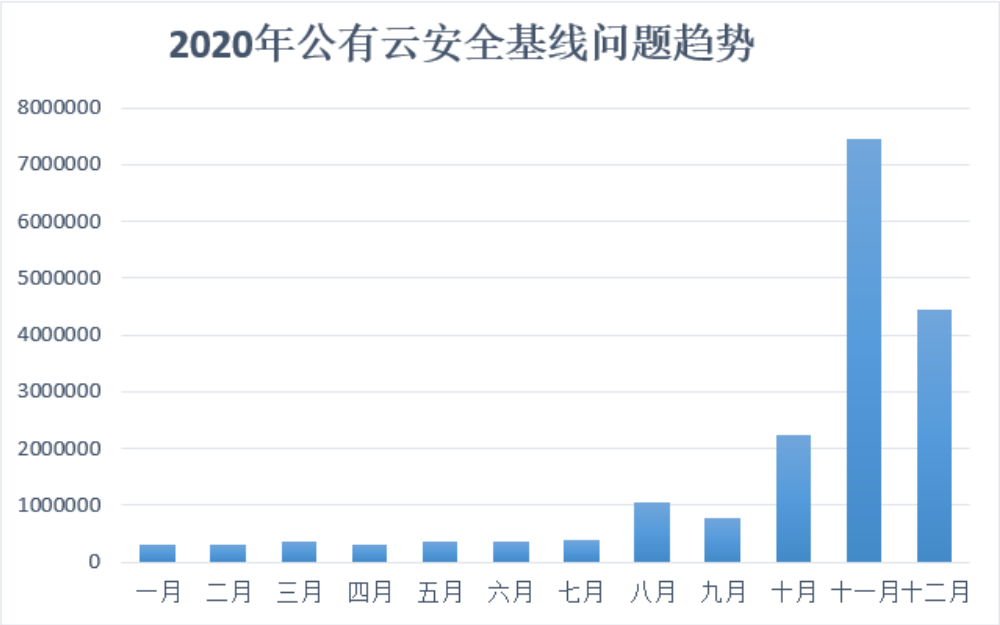


图 14

## 6.2 安全基线问题 Top

主要存在的安全基线风险为限制 root 权限用户远程登录、Linux 口令过期后账号最长有效天数策略和 Linux 帐户超时自动登出配置。

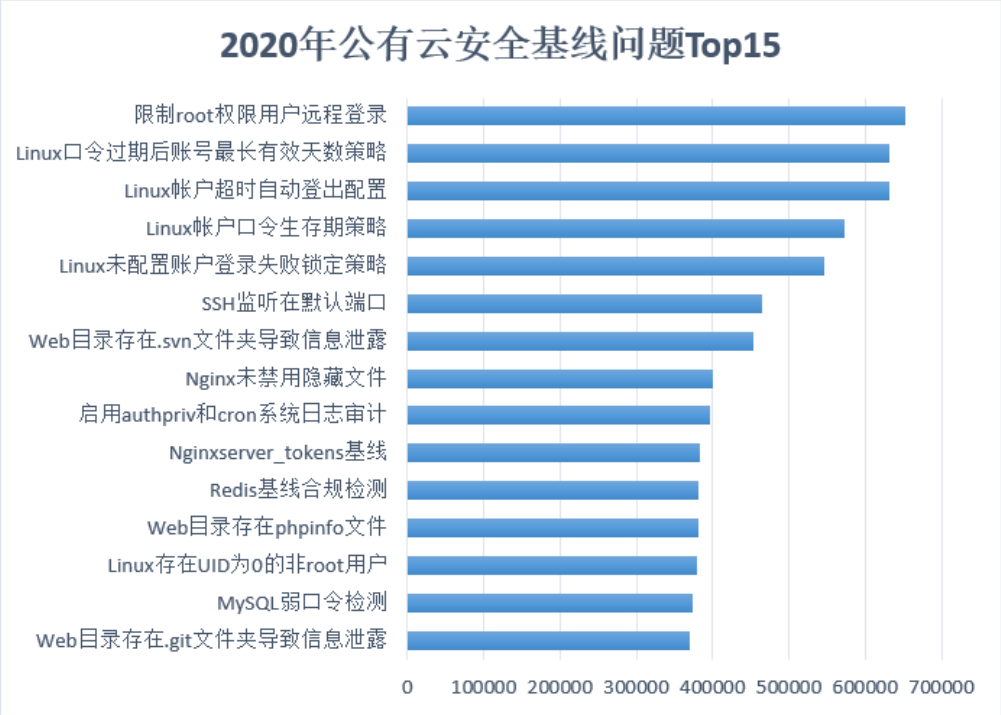


图 15

## 6.3 安全基线风险等级

通过基线检测，发现政企机构云上业务存在高中危以上风险的达到 83%，可以说云上资产安全现状不容乐观。

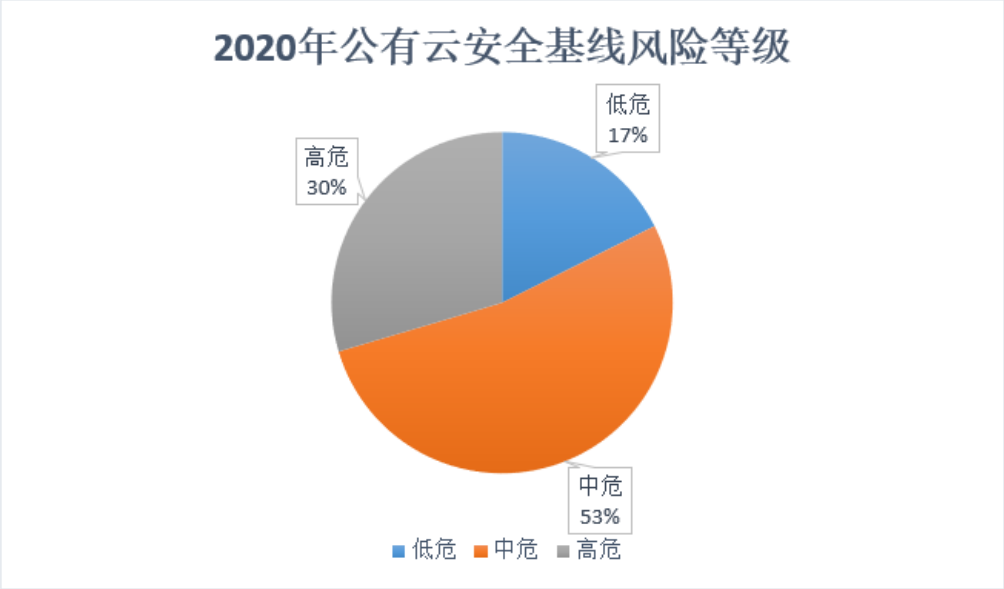


图 16

## 6.4 安全基线风险利用典型案例

### Mirai 僵尸网络针对 Linux 服务器的 SSH（22 端口）进行弱口令爆破攻击

腾讯安全威胁情报中心检测到 Mirai 僵尸网络大规模攻击 Linux 服务器。攻击者针对 Linux 服务器的 SSH（22 端口）进行弱口令爆破攻击，成功登陆后执行 shellcode 下载 shell 脚本，然后通过 shell 脚本依次下载基于多个系统平台的 Mirai 僵尸网络二进制木马程序。

Mirai 是一个大型僵尸网络，主要通过 SSH 和 telnet 弱口令进行感染，攻击目标包括监控摄像头、路由器等物联网设备以及 Linux 服务器，控制机器后通过 C&C 服务器下发命令进行 DDoS 攻击。根据腾讯安全威胁情报中心监测数据，Mirai 僵尸网络已在全国造成上万台设备感染，其中感染最多的为广东、上海和北京。

参考链接：https://mp.weixin.qq.com/s/8yTiVyxC6_aapGhrTs1uWw

### 挖矿木马 BasedMiner 针对 MS SQL 服务进行爆破弱口令攻击

腾讯安全威胁情报中心检测到针对Windows服务器进行攻击的挖矿木马BasedMiner。该挖矿木马团伙主要针对 MS SQL 服务进行爆破弱口令攻击，爆破成功后会下载 Gh0st 远控木马对系统进行控制，还会利用多个 Windows 漏洞进行提权攻击获得系统最高权限，最后植入门罗币挖矿木马进行挖矿，目前已获利 8000 元。

因其远控模块名为 based.dll，腾讯安全中心将其命名为 BasedMiner。BasedMiner 入侵后在企业服务器植入远控木马，会导致受害企业机密信息泄露，挖矿时严重消耗服务器资源，会影响正常业务运行。腾讯安全专家建议企业检查纠正使用弱口令登录服务器，修复服务器存在的安全漏洞，避免挖矿团伙入侵。

参考链接：https://mp.weixin.qq.com/s/b9Nkl6q4xLoADNosP9jFkw

## 7、高危命令执行

高危命令有可能是黑客入侵之后，进一步执行恶意操作时执行的命令，也有可能是运维人员在日常操作时执行的有风险命令。需要运维人员针对高危命令的执行进行重点关注和审计，及时研判是主动执行、意外执行，或入侵者执行的可能。

执行的高危命令主要有设置操作命令不记录进日志、nc 命令执行和 wget 下载后执行命令等。


图 17

# 8、网络攻击事件

网络攻击指黑客从外网对云上主机进行入侵攻击，以及攻陷主机之后在内网进一步扩散的攻击行为。对于入侵成功的攻击，需要及时进行阻断，防止沦陷。

## 8.1 网络攻击趋势

从近三个月的趋势来看，网络攻击整体呈上升趋势。


图 18

## 8.2 网络攻击类型

在检测到的网络攻击事件中，主要为命令注入攻击。

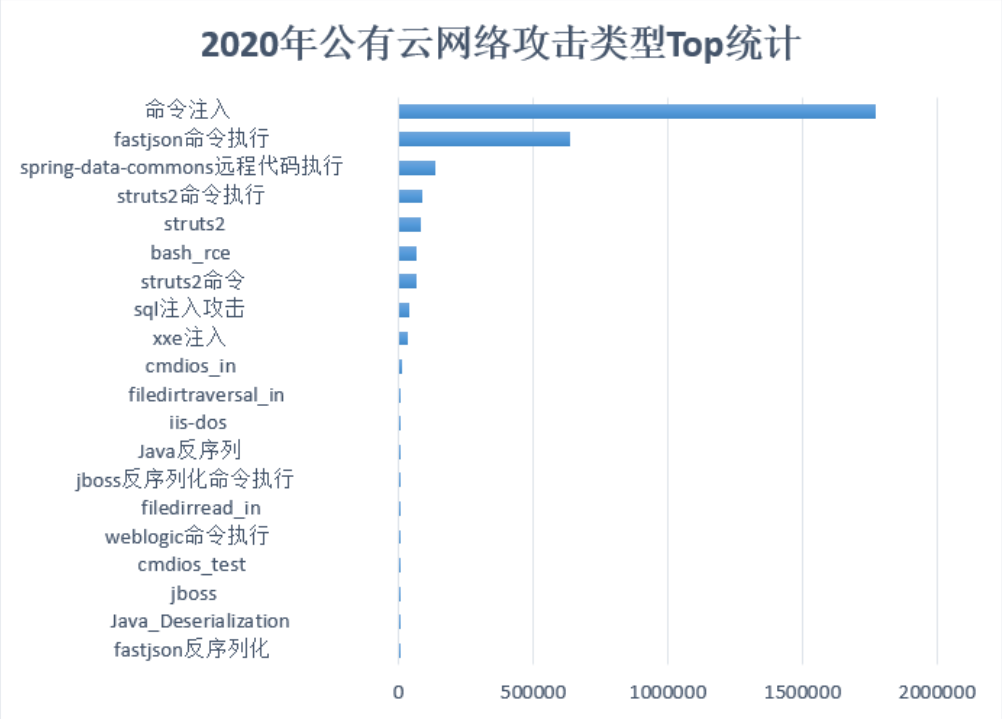


图 19

# 三、安全趋势

## 1、利用安全漏洞的云上攻击持续增加

近年可以发现，组件漏洞的披露越来越频繁；从各安全厂商发表的文章也可以发现，对漏洞的响应也越来越频繁。随着云上业务的发展，云上服务器使用的组件变得更加广泛。当组件存在漏洞时，便给了黑客入侵的有利途径，能够轻而易举突破防御攻陷主机。而另一方面，我们注意到政企机构对高危漏洞的修复速度并不乐观，给攻击者留下较多时间窗口。

## 2、安全基线风险日益凸显

相对于安全漏洞，企业安全运维人员对安全基线类问题的关注要弱许多，但基线问题却是黑客攻击最常利用的管理漏洞。例如当主机登录密码使用了默认口令、弱口令时，黑客能够轻易通过爆破登录主机执行恶意操作。安全基线能够有效提高黑客的入侵门槛，建议运维人员严格按照安全规范进行配置，同时让企业云上资产安全符合国家等保合规要求。

## 3、定向攻击更为普遍

在 2020 年 10 月，腾讯主机安全捕获多起云上针对游戏行业的 APT 攻击。在以往 APT 更多的会针对国家重点单位进行攻击，如今在多个行业里均开始出现了 APT 攻击的身影。针对游戏行业的 APT 攻击，往往会窃取游戏源码、机密资料等信息，将会给游戏开发企业带来严重风险。

2020 年连续发生连续震惊全行业的 APT 攻击事件：Fireeye 遭遇 APT 攻击红队工具

被盗；SolarWinds 供应链攻击影响美国众多知名企业及政府机关。预计，2021 年针对重点目标的网络安全形势仍然不容乐观。

## 4、挖矿木马广泛传播

挖矿木马在云上攻击事件中是最为流行的安全事件之一。一旦主机被传播挖矿木马之后，挖矿木马会占用大量主机资源，进而影响业务正常运行。此外挖矿木马团伙还是同时部署、携带横向传播模块，一旦个别系统失陷，可能导致企业批量主机失陷，企业损失会迅速增加。因此发现主机挖矿木马时需要及时查杀，并且定位失陷原因进行漏洞修复。

## 5、云上勒索病毒攻击仍需重点防范

云上攻击攻击事件中，勒索病毒攻击依然流行。勒索病毒会通过加密主机上的数据文件来勒索巨额赎金，否则业务将会受到严重影响，甚至停摆。建议运维人员定期备份重要数据资料，防止数据丢失后无法找回。

# 四、安全建议

## 1、主机安全

建议全网安装部署终端安全管理软件，企业管理员可以通过这些安全解决方案及时发现内网入侵风险，及时封堵弱点，修补漏洞，建议由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略、软件限制策略，以保证网络的动态安全。

## 2、重点服务器的保护

建议对重要的网络服务进行远程访问策略配置、对管理节点进行限制，只限定允许的 IP 地址访问管理后台。数据库服务避免使用弱密码，配置最大错误登录次数，防止远程黑客进行暴力破解。

安全运维团队通过部署腾讯 T-Sec 安全运营中心、腾讯 T-Sec 高级威胁检测系统密切注意异常告警信息，及时对告警进行分析处置，发现全网安全弱点，针对弱点因素进行重点修复防护，通过腾讯 T-Sec 云防火墙部署云主机访问控制策略，将威胁横向扩散的风险降到最低。

## 3、权限管控

从企业生产专有云网络向企业公有云资产“横向移动”，呈现出 APT 攻击的新特点。随着企业业务上云正在成为发展新趋势，相关企业需要建设专有云和公有云网络边界防护体

系，避免出现安全短板。

在企业内网向公有云的“横向移动”过程中，不安全的权限控制成为最主要的防御短板，尤其是 IT 运维权限，一旦被渗透，则会造成严重的数据资产损失。腾讯安全为客户提供了零信任无边界访问控制系统（iOA）体系来解决权限管控问题，在企业办公网和云上生产网之间，增加一道坚实的防护屏障。