Portmap反射DDoS爆发，阿里云平台自动检测识别并拦截

阿里云安全技术 / 2018-09-16 14:38:44 / 浏览数 3563 技术文章 技术文章 顶(0) 踩(0)

阿里云安全团队于2018年9月14日0:10分监控到一起大规模攻击事件，当天近3000台的Portmap服务器被利用来进行反射DDoS攻击，平均反射放大比均值在7.X。阿里云平

事发当日，仅阿里云安全团队拦截的从平台流出的对外Portmap攻击流量最高或可达到57G，预计全网该反射的攻击流量更是一个天文数字，危害极大。同时，被利用来反射

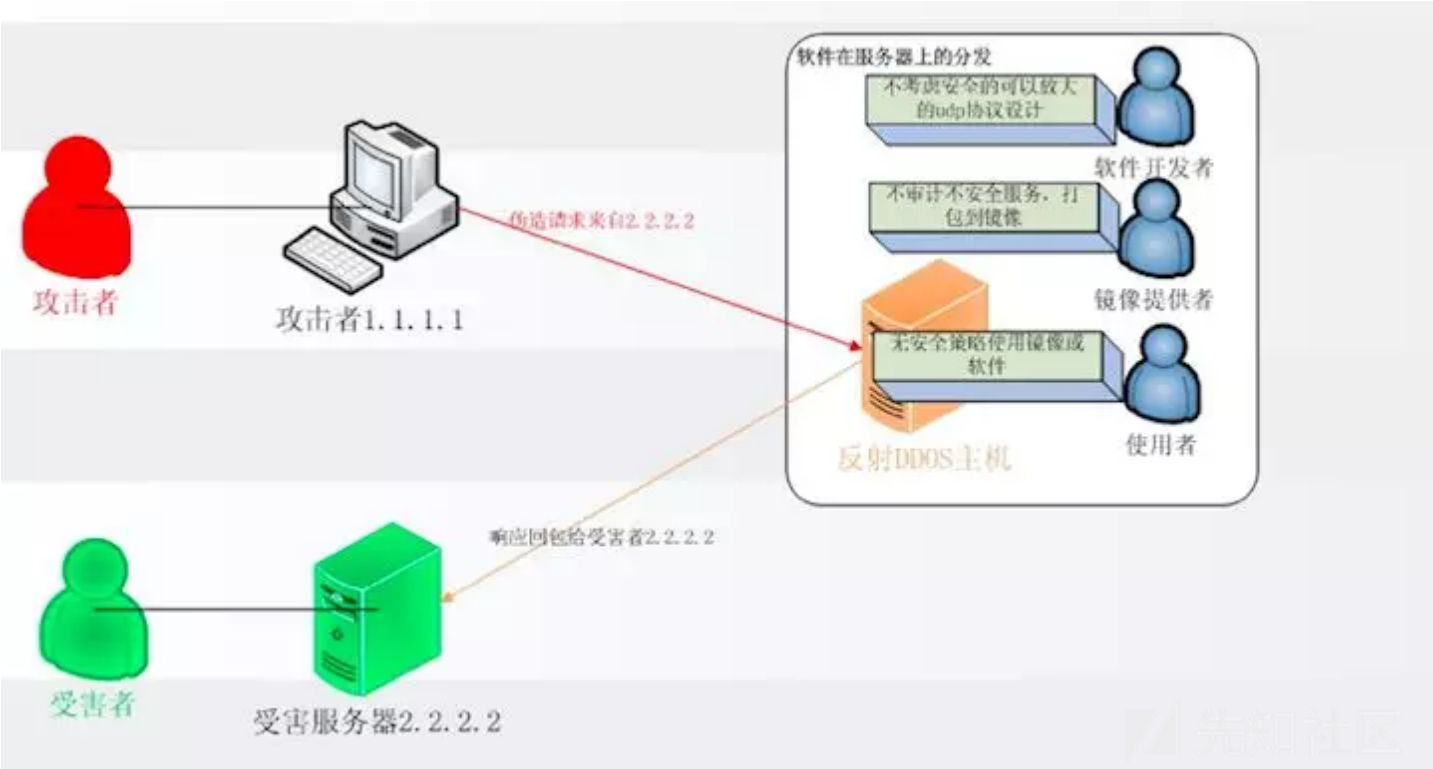
阿里云安全团队建议用户关注服务器上是否有开启RPCBind服务，如果业务中并没有使用RPCBind，可直接关闭，避免您的服务器被利用导致的业务受影响。

详细分析如下：

Portmap反射DDOS的成因

Portmap RPCBind服务在TCP或UDP的111端口上运行，对该服务发起一个普通查询需要68字节，服务器响应包486字节，反射放大比为7.14。

一般反射DDOS攻击原理如下图所示：



反射DDOS实施的2个必备条件：

可以伪造源IP。

UDP协议无需连接，服务器响应包的大小远大于请求包大小，攻击以小博大。

针对以上数据流，我们认为限制并阻止违造源IP数据包发送到网络上，可以从根本上杜绝反射DDOS发生。

软件在服务器上的分发使用，我们认为：
a. 对“软件开发者”在设计服务时，需要有安全考虑，UDP协议存在放大时，可以加入鉴权机制。
b.对“镜像提供者”，在打包软件进入镜像时，默认镜像应审计其安全，不安全的打包安全策略。
c. 对“使用者”，在使用优先使用需要建立连接的TCP的服务，禁用UDP，以免在未建连接情况下伪造IP被以小博大。

全网情况

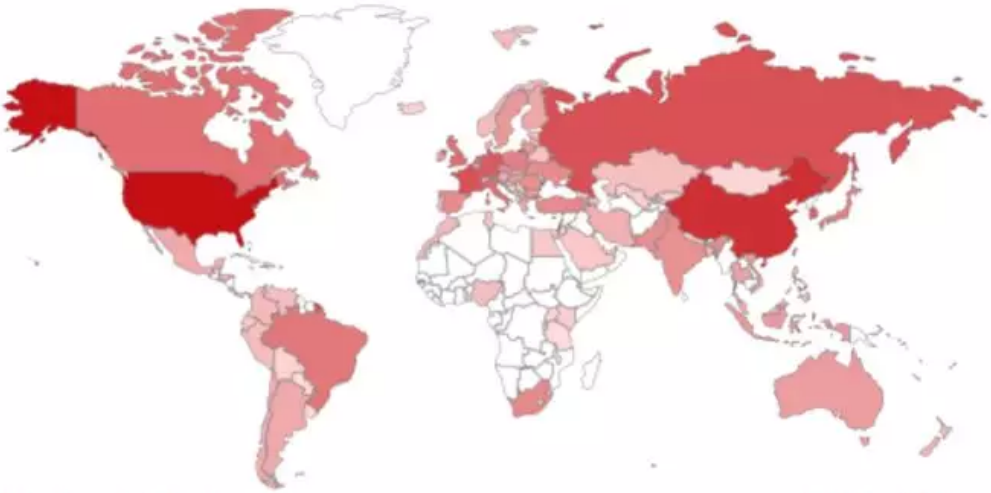
在shodan上搜索，整个互联网上潜在被利用的攻击主机数量近两百万，如下图：

Exploits Maps

TOTAL RESULTS

2,056,710

TOP COUNTRIES



United States	598,699
China	299,881
Russian Federation	129,118
France	123,311
Germany	95,101

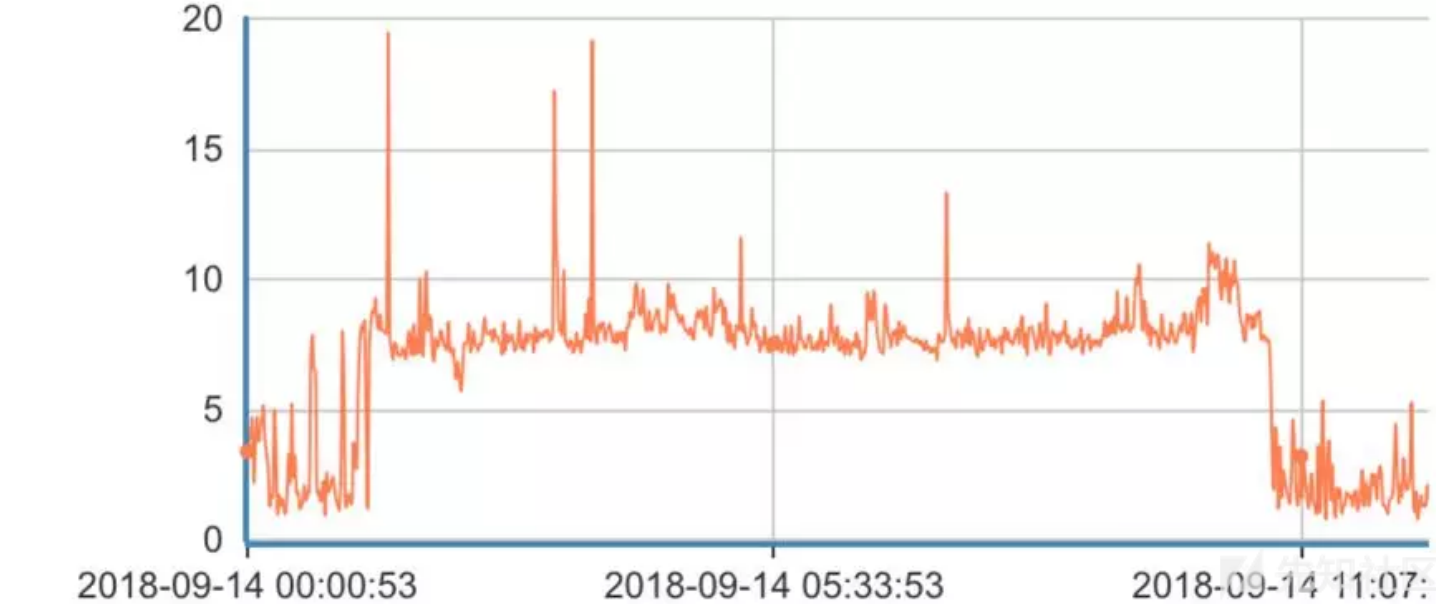
TOP SERVICES

Portmap	2,056,704
5672	3
Oracle	2
Telnet (Lantronix)	1

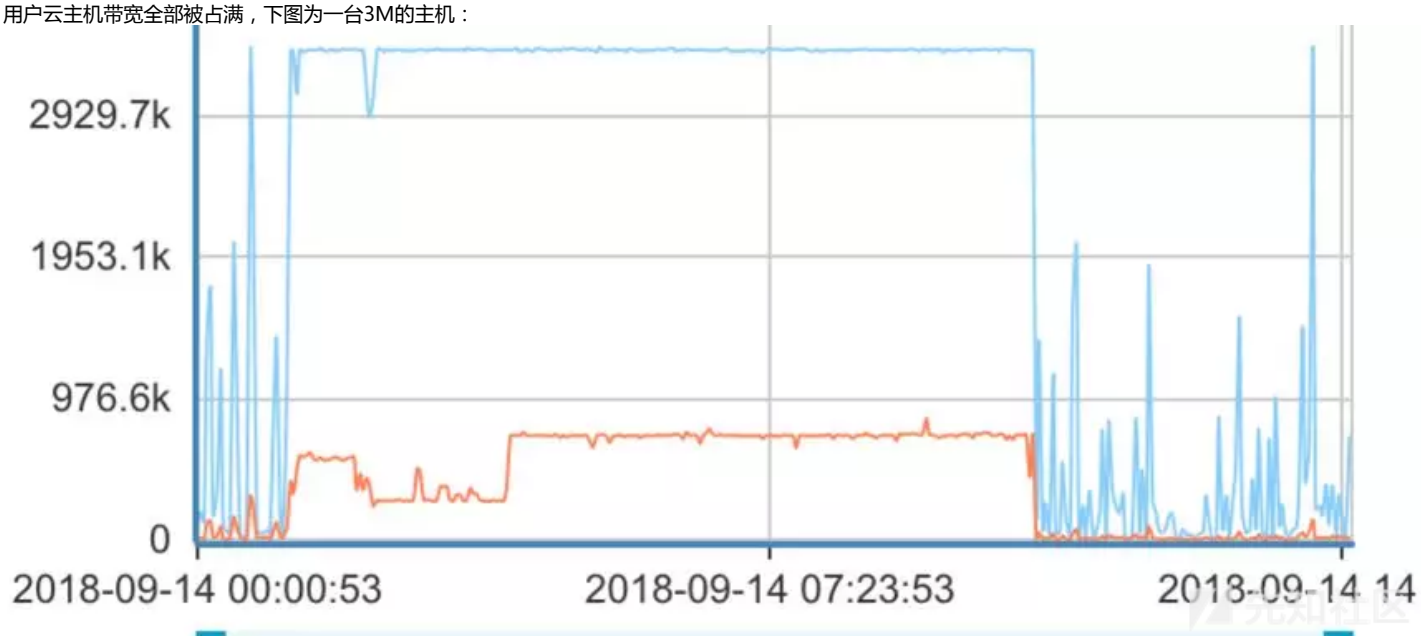
（数据引用自shodan）

Portmap反射DDOS的危害

- 用户云主机的CPU占用率会比日常高出几倍



- 用户云主机带宽全部被占满，下图为一台3M的主机：



阿里云平台对反射DDOS自动管控：

处理时间快：9月14日首次Portmap攻击事件在00：10发生，全天共发现Portmap事件4000余起，涉及IP数2700余个，30s内完成检测并自动进行管控。

用户影响小：平台不关停用户云主机，对攻击流量进行管控，基本对用户正常业务无影响。

检测类型广：包含Portmap在内，平台检测并处置9种反射DDOS类型。

反射 DDOS 类型	通知方式	处置方式	云内流行程度
Qotd	站内信	管控对外访问 UDP	低
Ntp	站内信	管控对外访问 UDP	中
Dns	站内信	管控对外访问 UDP	低
Portmap	站内信	管控对外访问 UDP	高
Chargen	站内信	管控对外访问 UDP	高
Snmp	站内信	管控对外访问 UDP	低
Ssdp	站内信	管控对外访问 UDP	低
Memcache	站内信	管控对外访问 UDP	高
Cldap	站内信	管控对外访问 UDP	高

UDP各种服务的反射放大比如下图，引用自美国CERT公布的数据

https://www.us-cert.gov/ncas/alerts/TA14-017A：

Protocol	Bandwidth Amplification Factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP [7]	56 to 70
TFTP [23]	60
Memcached [25]	10,000 to 51,000

用户应急建议：

直接关闭RPCBind服务：如果业务中并没有使用RPCBind，可直接关闭。

Ubuntu：

(1) 打开终端，运行如下命令，关闭RPCBind服务：

sudo systemctl stop rpcbind.socket

(2) 检查RPCBind服务是否关闭:

netstat -anp | grep rpcbind

CentOS：

(1) 打开终端，运行如下命令：

systemctl stop rpcbind.socket

(2) 检查RPCBind服务是否关闭：

netstat -anp | grep rpcbind

上一篇：sqlmap的使用 ---- 自带... 下一篇：从一道ctf题目学到的绕过长度执行...

1. 0 条回复
   - 动动手指，沙发就是你的了！