黑客反制之路-大流量时代的DDoS防护

钱华钩 百度安全

2021 SDC分会场-公开课

议题目录

第一章 新型攻击层出不穷

PC端

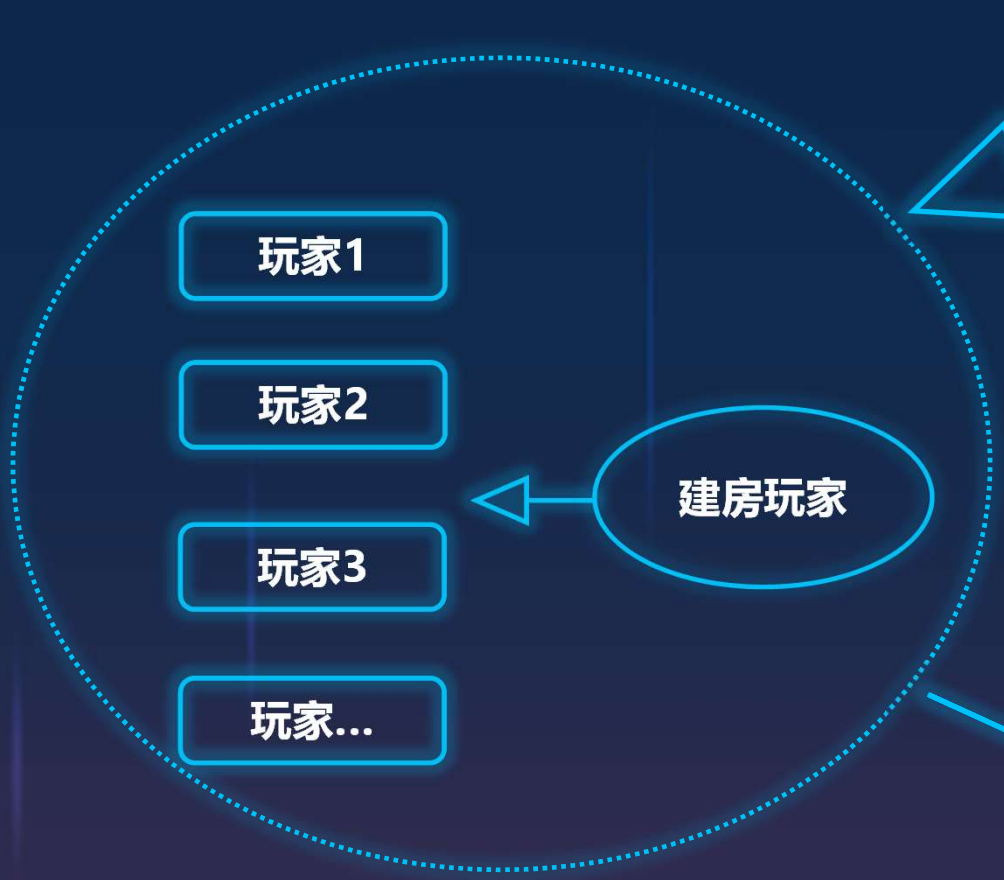
IoT设备

手机客户端

透过攻击流量，我们看到大量的攻击来自于PC、IoT、手机客户端

你是否是黑客的一个帮凶?

隐藏在游戏中的DDoS攻击



黑客
获取房间信息等配置

A2S_INFO协议问题：

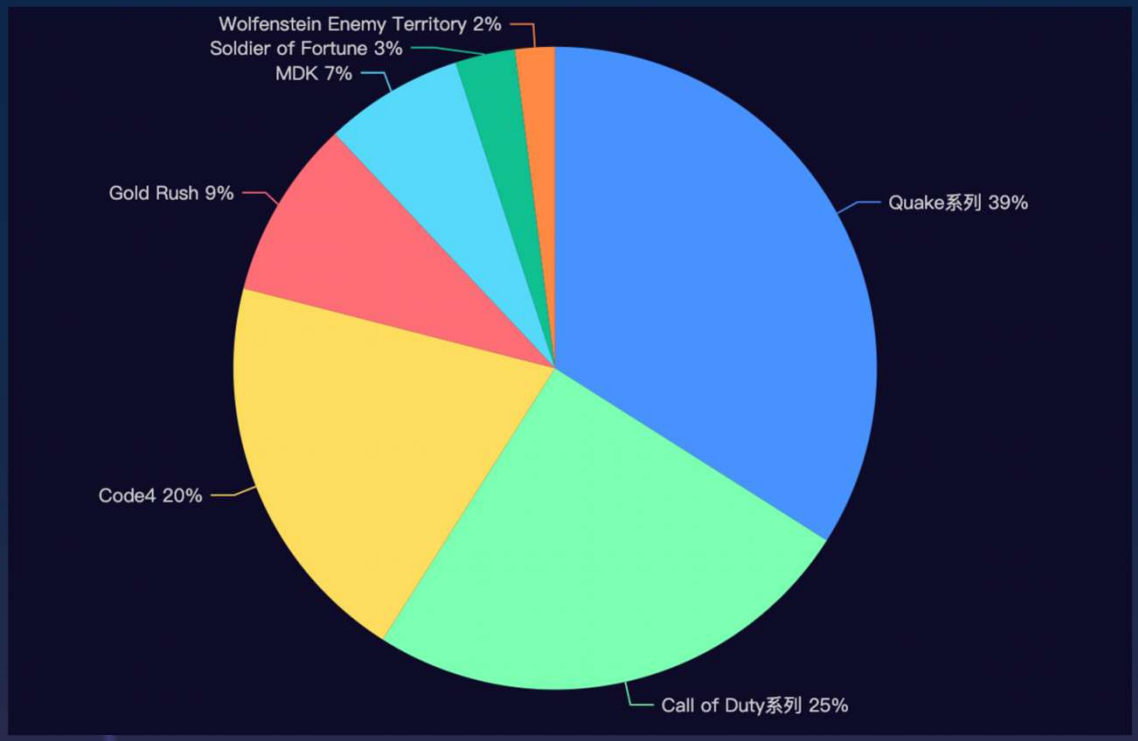
- 所有的玩家上线会开放端口
- 开放端口的列表能够被查到
- 开放端口可以随意请求
- 响应数据包大于请求包

受害者

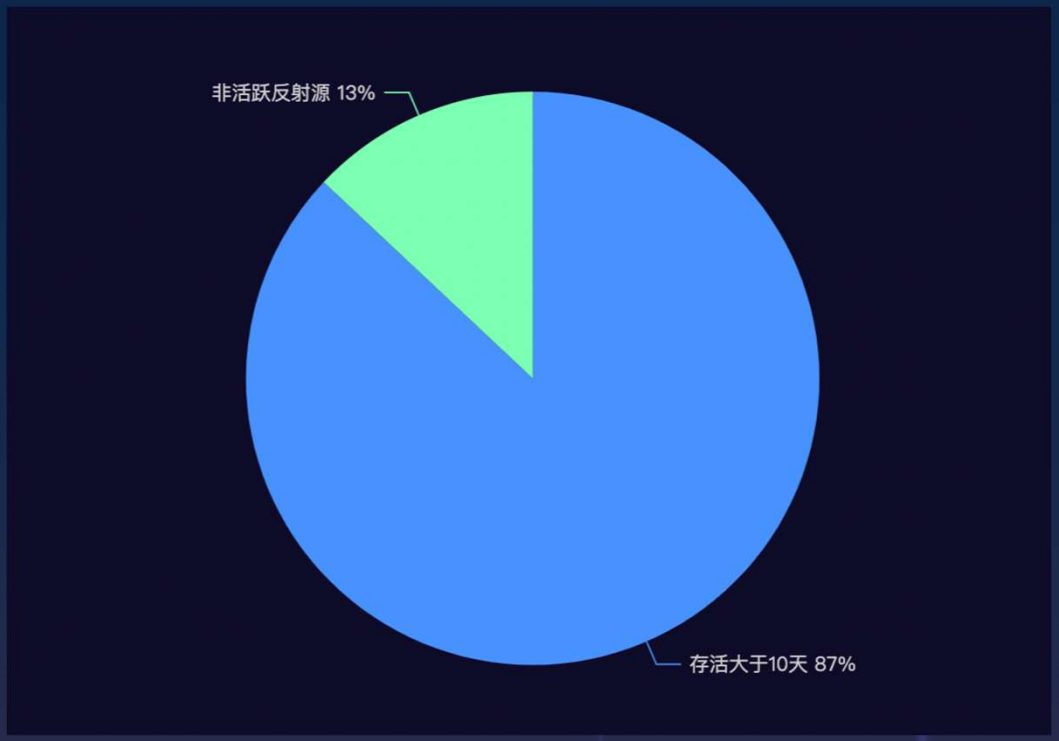
Steam游戏P2P网络

——《DDoS新领域 隐藏在游戏里的反射源》

很多对战类游戏都可能成为黑客发起反射攻击的帮凶



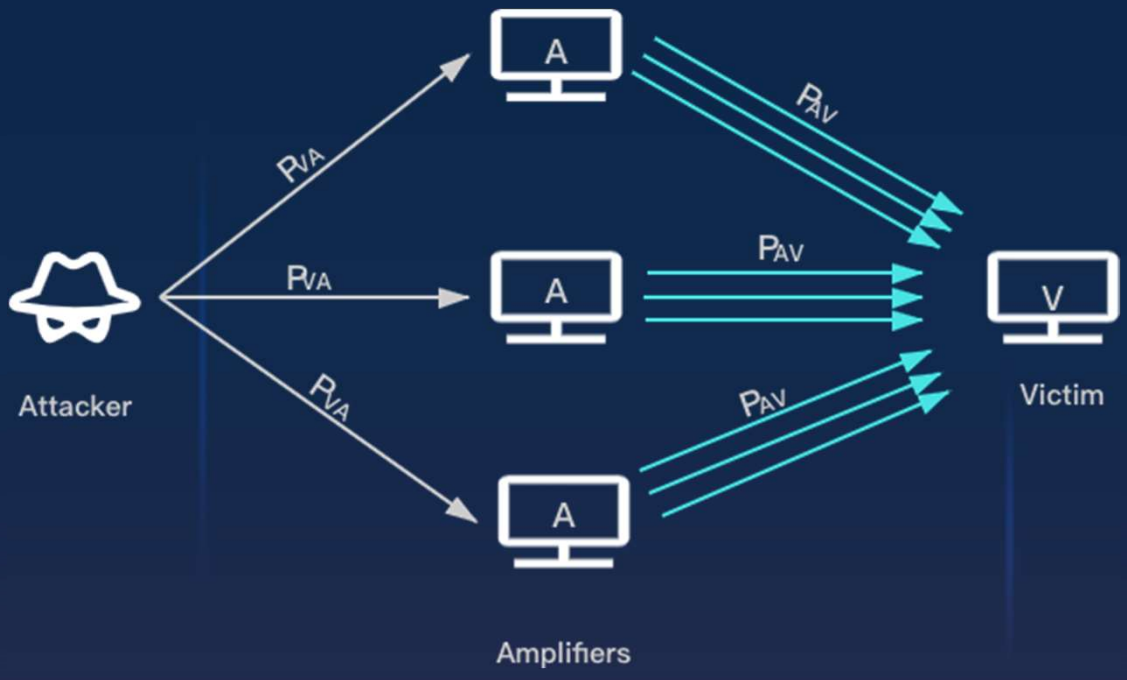
游戏类型占比



存活时间占比

——《DRDoS预警：那些被黑客盯上的对战游戏》

反射攻击原理



三个角色：

Attacker【攻击者】、Amplifiers【反射服务器】、Victim【目标服务器】

两个过程：

攻击者伪造了一批请求包Pva，发送到反射服务器

反射服务器发送大量的响应包Pav指向目标服务器。

两个特征：

反射流量

放大流量

反射攻击的放大倍数

5万倍 CF在2018年2月发布文章称，捕获5万倍的Memcached DRDoS攻击。 $\frac{\text{响应数据750kB}}{\text{请求数据15B}}$ = 5万倍

802.3 以太网帧结构

前导码	帧开始符	MAC 目标地址	MAC 源地址	802.1Q 标签 (可选)	以太类型	负载	冗余校验	帧间距
10101010 7个octet	10101011 1个octet	6 octets	6 octets	(4 octets)	2 octets	46—1500 octets	4 octets	12 octets
		64—1522 octets						
72—1530 octets								
84—1542 octets								

以太网数据包包头：14+20+8+24 = 66

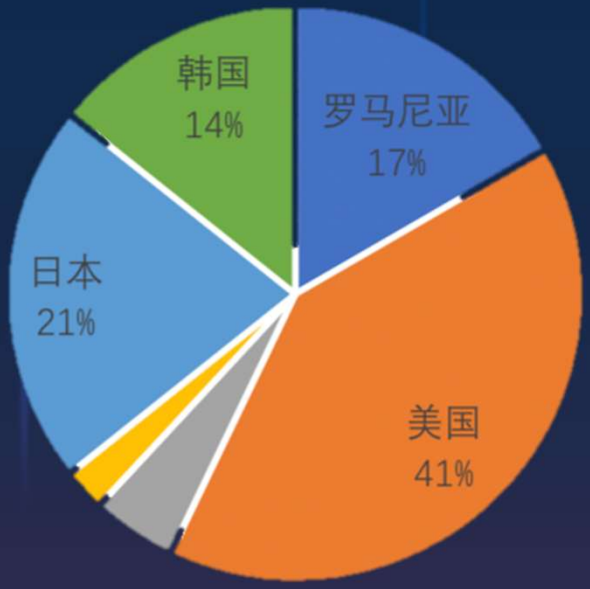
按照CF数据重新计算：
响应数据流：750*1024/1400*(1400+66) = 804205.7
请求数据流：最小包84
实际放大倍数：804205/84 = 9573.9 倍。

捕获攻击变种最大反射倍数： 15万倍
205个get a\r\n
1024*1024*205/1400*1466/1509= 149166.2倍!

——《Memcached DRDoS攻击趋势》

黑客自建反射源的攻击

全网扫描结果



反射特点

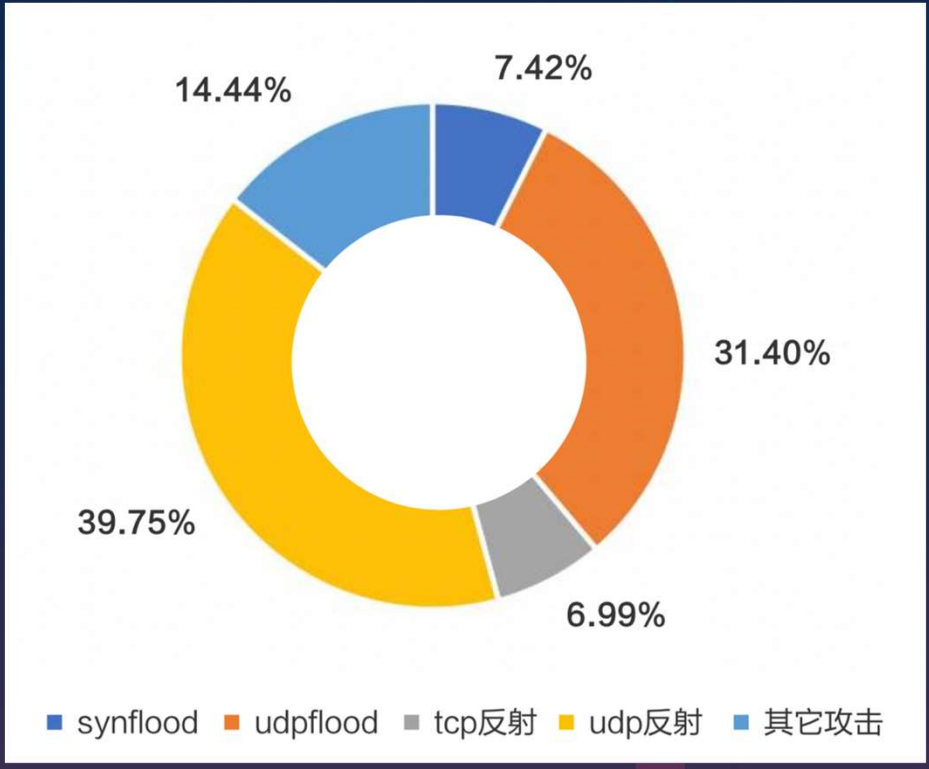
- 发送最小的数据包
- 返回2325个1370大小的包
- 反射倍率4万倍

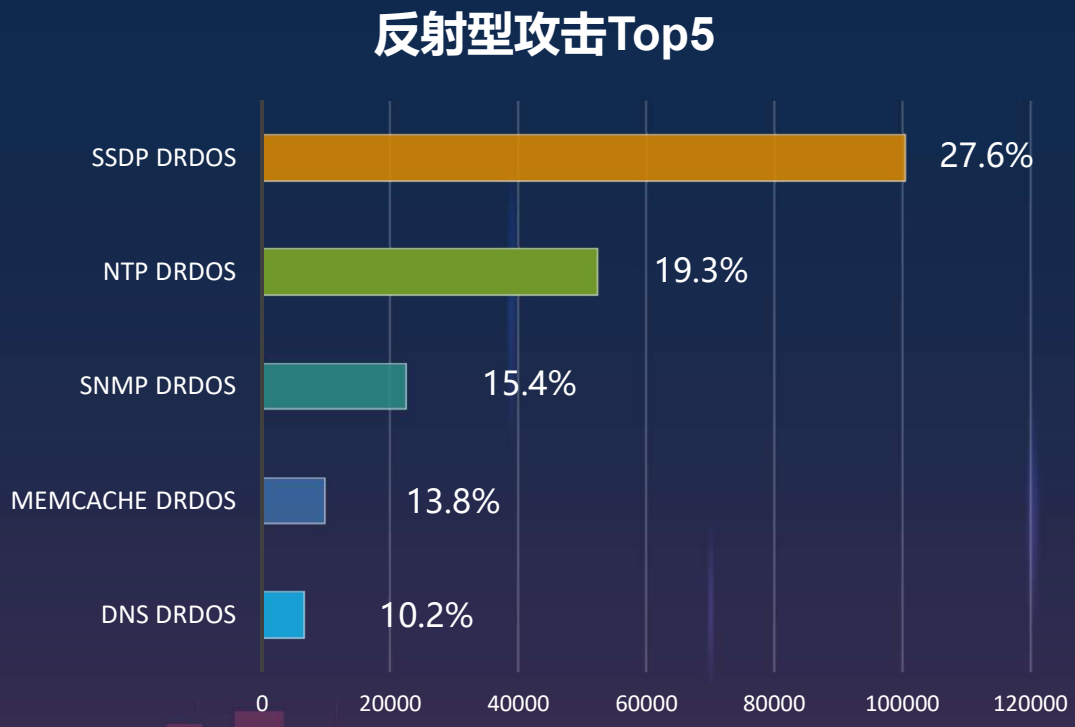
No.	Time	Source	Destination	Protocol	Length
36	3.238646	172.18.4.163	[redacted]	UDP	43
37	3.490180	[redacted]	172.18.4.163	UDP	1370
38	3.493831	[redacted]	172.18.4.163	UDP	1370
39	3.496885	[redacted]	172.18.4.163	UDP	1370
40	3.500631	[redacted]	172.18.4.163	UDP	1370
41	3.501845	[redacted]	172.18.4.163	UDP	1370
42	3.504866	[redacted]	172.18.4.163	UDP	1370
43	3.508043	[redacted]	172.18.4.163	UDP	1370
44	3.509950	[redacted]	172.18.4.163	UDP	1370
45	3.512046	[redacted]	172.18.4.163	UDP	1370
46	3.514167	[redacted]	172.18.4.163	UDP	1370
47	3.517857	[redacted]	172.18.4.163	UDP	1370
48	3.520656	[redacted]	172.18.4.163	UDP	1370
49	3.523061	[redacted]	172.18.4.163	UDP	1370
50	3.526103	[redacted]	172.18.4.163	UDP	1370
51	3.529105	[redacted]	172.18.4.163	UDP	1370

——《威胁预警：首次监控到黑客自建数万倍的反射源参与反射攻击》

反射攻击已经成为主流

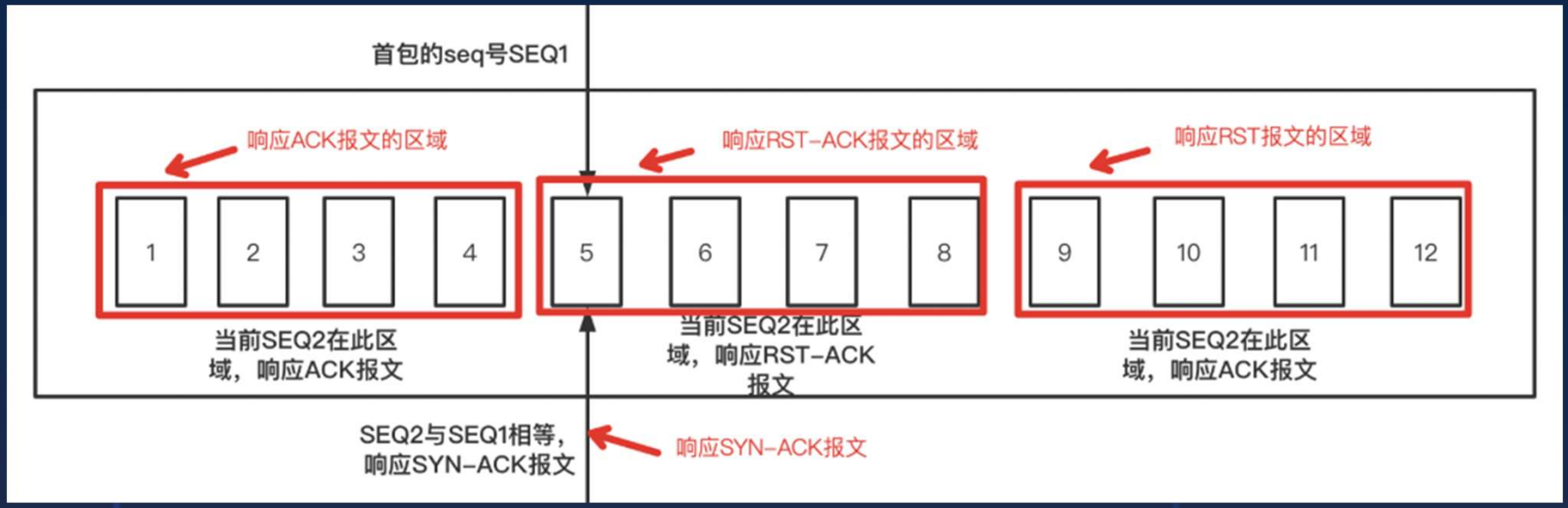
- 反射类攻击已经占比接近50%
- SSDP、NTP、DNS、CLDAP和Memcached 占据了UDP反射的Top5， 占比超过75%





——数据来源于百度安全联合联通云盾《2020年DDoS攻击态势报告》

TCP反射攻击



反射方式

- SYN-ACK 反射
- ACK 反射
- RST-ACK 反射
- RST 反射

反射特点

- 反射源多
- 难以防御
- 类型复杂易穿透

——《DRDoS预警：TCP反射的深度分析》

新型反射攻击研究方法

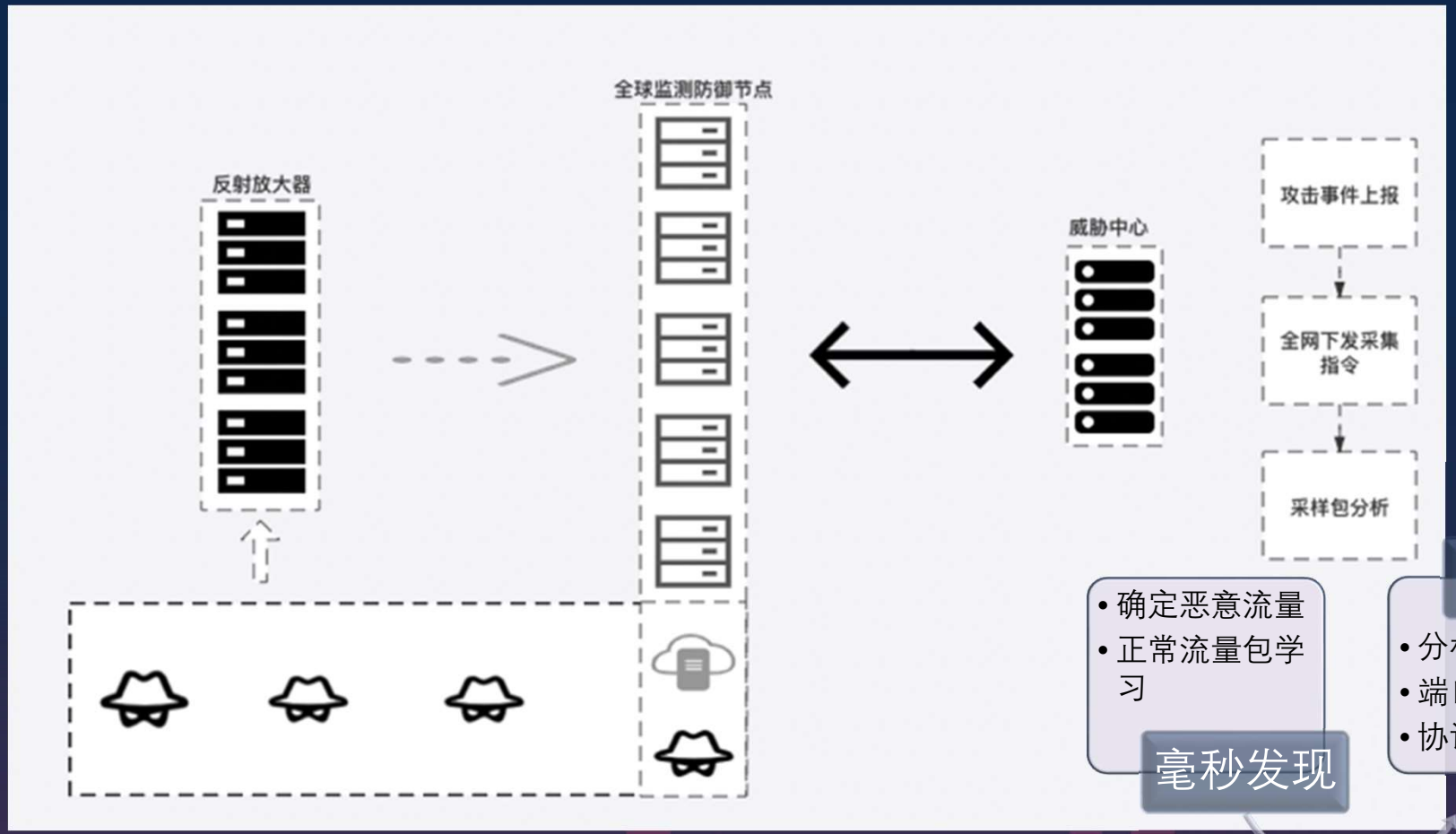
捕获

部署蜜罐和攻击采样未知流量，分析定位

FUZZ

结合反射攻击原理从RFC协议中模糊测试，定位新的攻击手法

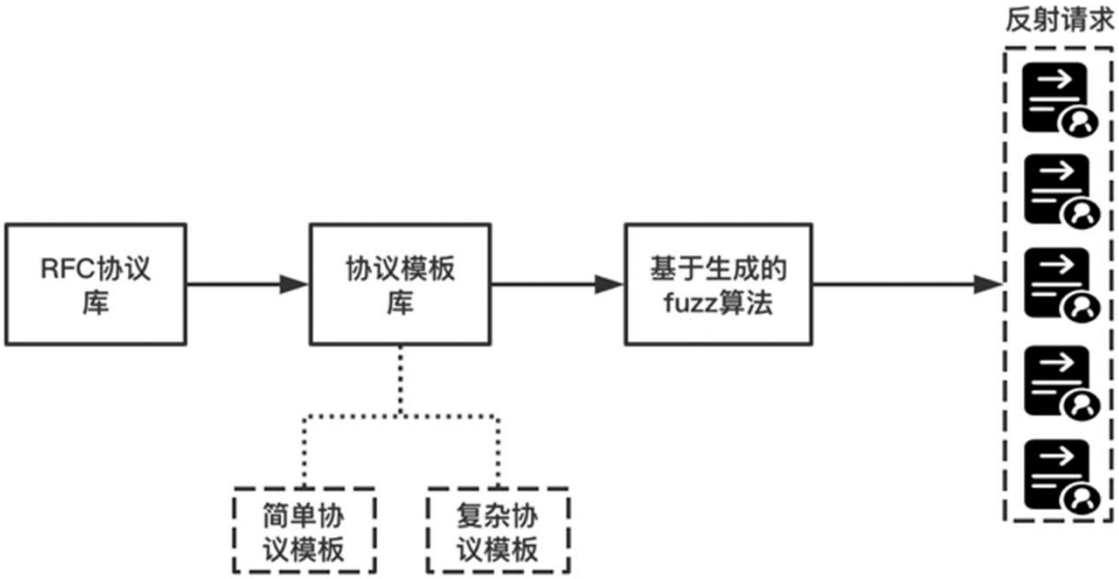
捕获新型DDoS 0day攻击



——《DDoS攻击愈演愈烈，反射攻击举足轻重》

FUZZ新型DDoS 0day攻击

结合反射攻击原理从RFC协议中模糊测试定位新的攻击手法



- 罗列RFC中基于UDP的协议
- 收集网络上相应的开放服务
- 构建协议请求模板
- FUZZ大量请求包
- 响应数据包分析
- 定位攻击手法

——《DDoS攻击愈演愈烈，反射攻击举足轻重》

捕获新型DDoS 0day攻击

一种利用SmartZone网络控制器的DDoS反射放大攻击

7月19日，Ruckus公司发布公告，宣称修复了SmartZone系列产品的重大安全漏洞。

百度安全实验室　已有12208人围观　2021-07-24

黑客团伙GuardMiner的挖矿之路

针对云上主机的恶意挖矿行为呈现上升趋势，最常见的挖矿币种就是门罗币。

百度安全实验室　已有143478人围观 · 发现5个不明物体　2021-06-11

DRDoS预警：WdbRPC与BACnet协议可被反射攻击利用

团队在进行大量的UDP协议分析时，发现了两类协议可以被利用作为反射放大攻击。

百度安全实验室　已有114047人围观 · 发现1个不明物体　2021-05-21

DDoS预警：TCP反射的深度分析

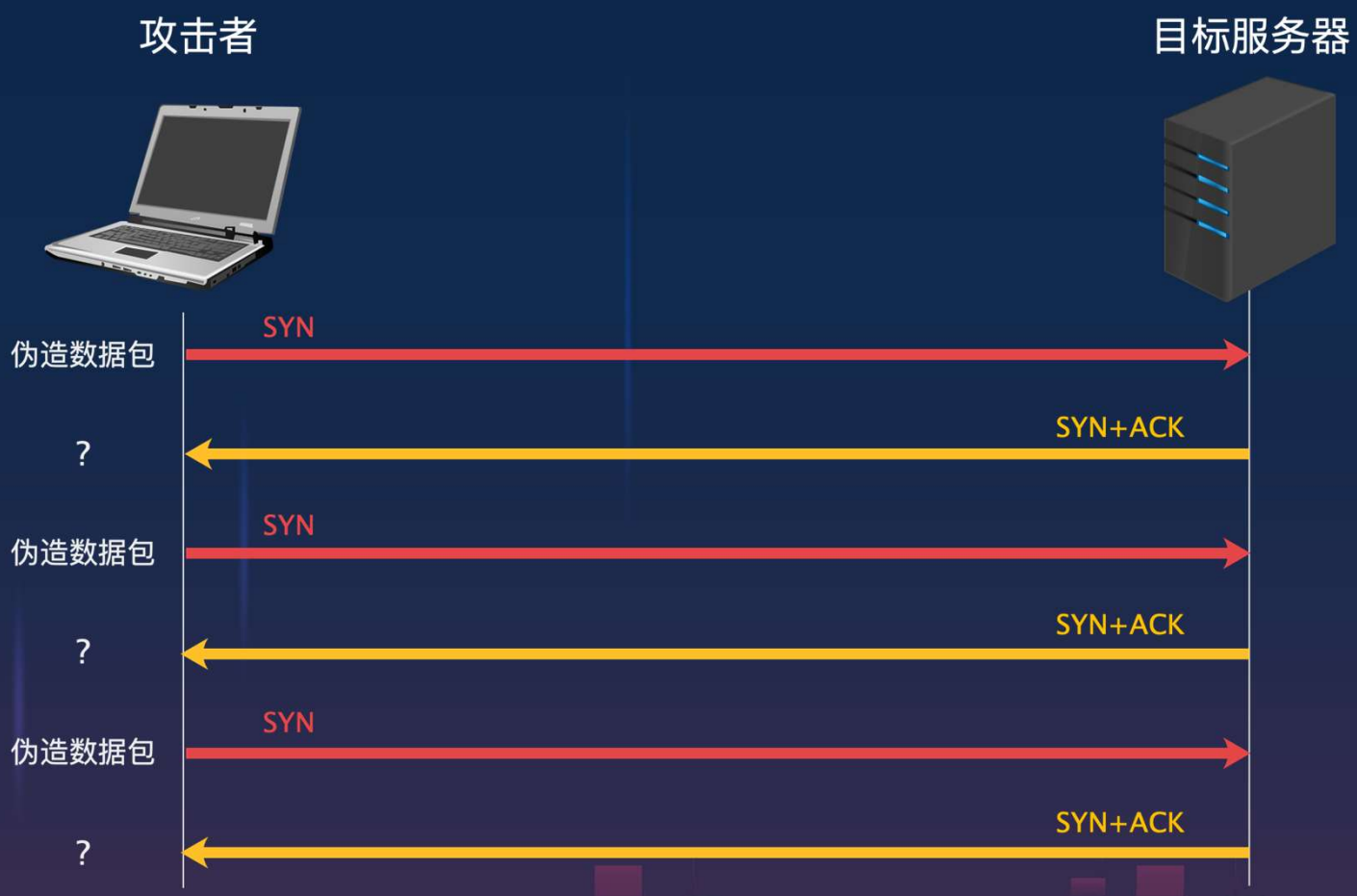
TCP反射攻击是在现网的DDoS攻防对抗中，逐渐兴起的一种新型攻击方式。

全球首次
捕获 13 种新型攻击

- IPMI反射
- CoAP反射
- OnVIF反射
- FLex反射
- SmartZone反射
- A2S_INFO反射
- WSD反射
- DTLS反射

第二章 DDoS防御最佳实践

最小的DDoS攻击



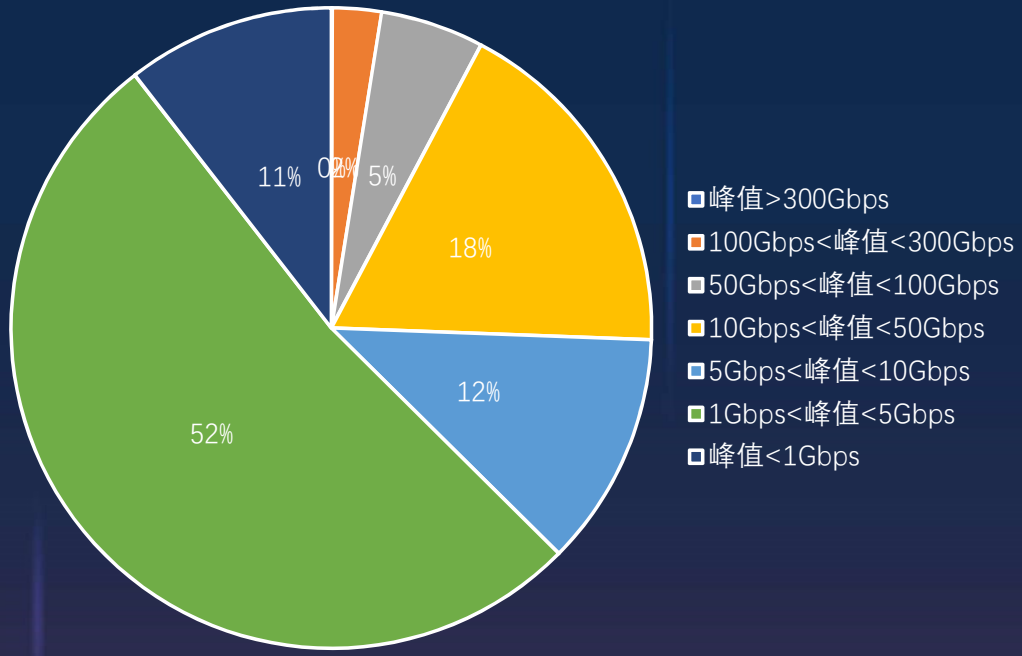
1个syn包 84字节

1Mbps/8/84 = 1488个包

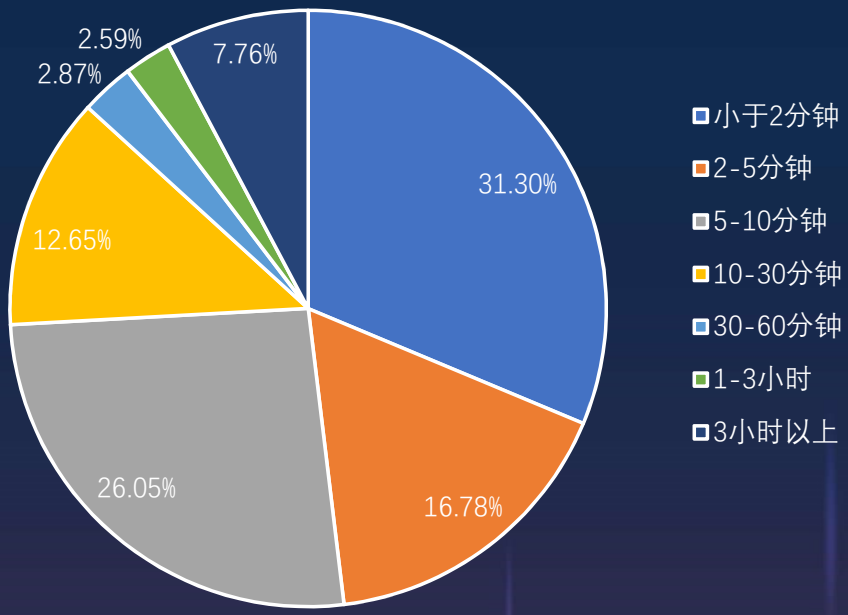
全网DDoS攻击年度峰值趋势

2021 SDC

2020年 攻击峰值占比分布



2020年 攻击时长占比



5G以下的流量攻击占比超过60%

——数据来源于百度安全联合联通智慧《2020年DDoS攻击态势报告》

三四层流量攻击防御实践

在没有堵死网络出口的情况下，少量DDoS攻击仍然瘫痪业务系统

三、四层DDoS

攻击危害

典型特征

网络中充斥着大量无用数据包

主机上有大量等待的Tcp连接

CPU或内存占用率出现明显增长

访问卡顿、用户掉线

攻击应对

策略与效果

Linux服务内核开启Syn Cookie

-- Syn flood攻击会被cookie校验

防火墙关闭状态跟踪

-- Tcp反射数据包将被防火墙拦截

防火墙开启出向访问

-- 其他Tcp标志类flood将被协议栈丢弃

防火墙开启外部通用开放端口拦截

-- Udp反射和Flood都被防火墙拦截

防火墙开启入向目标80端口放行

-- Icmp 反射和Flood都被防火墙拦截

分布式拒绝服务分类

流量型攻击 DDoS

简单粗暴，通过海量流量堵死网络出口

- SYN Flood、ACK Flood、UDP Flood、FIN / RST Flood、ICMP Flood等

连接或内容攻击 CC

高RPS、大并发攻击网站动态请求，拖死主机、数据库资源

- 高并发攻击、连接耗尽、慢速攻击等，但攻击流量并不大

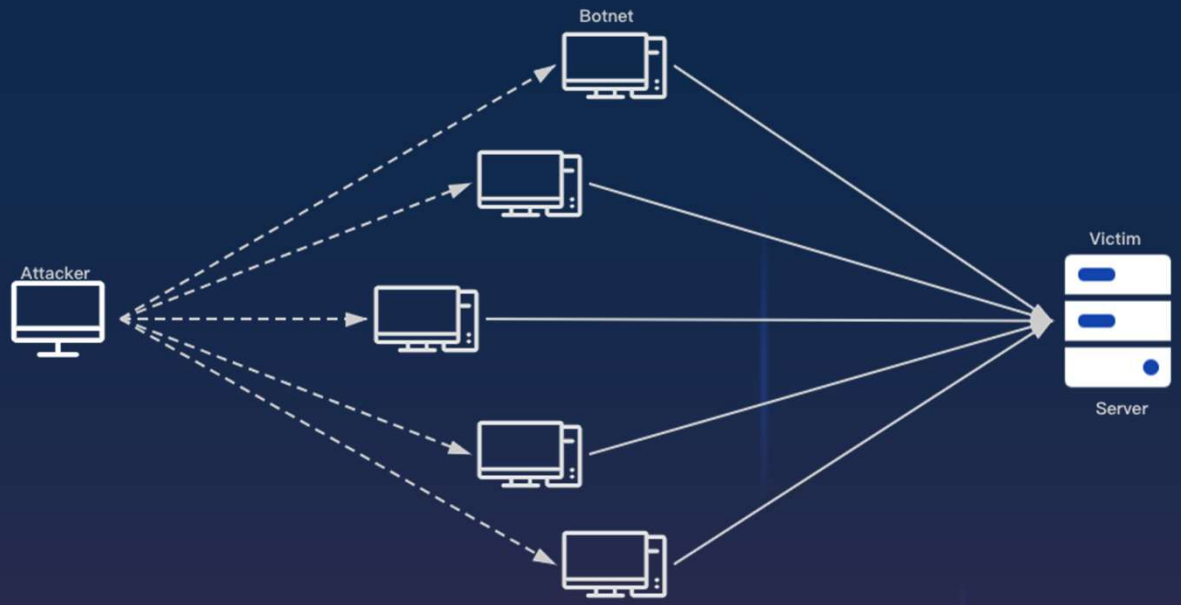
CC攻击简介

连接攻击

- 空请求
- 慢请求
- ACK请求

内容攻击

- WEB
- SSL
- DNS
- APP



CC攻击通常是高并发模拟正常用户，伪造成合法数据包访问网站，造成系统页面无响应、卡死。进而在线业务崩溃，带来海量用户投诉和巨额在线营收损失。

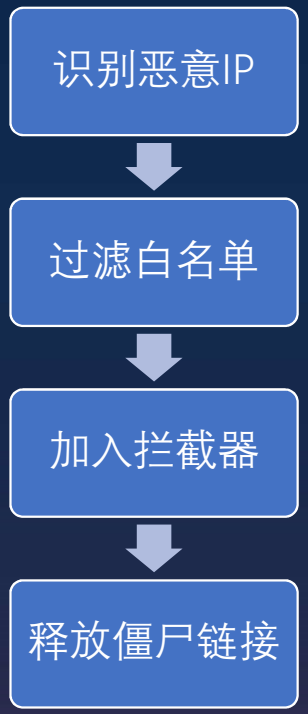
CC攻击的防御实践

典型特征

模拟正常请求访问

占用服务器的正常队列

频繁发生活动和重大节日期间



策略与效果

恶意IP（Botnet IP）识别

秒级拉黑恶意链接

释放僵尸链接

支持白名单

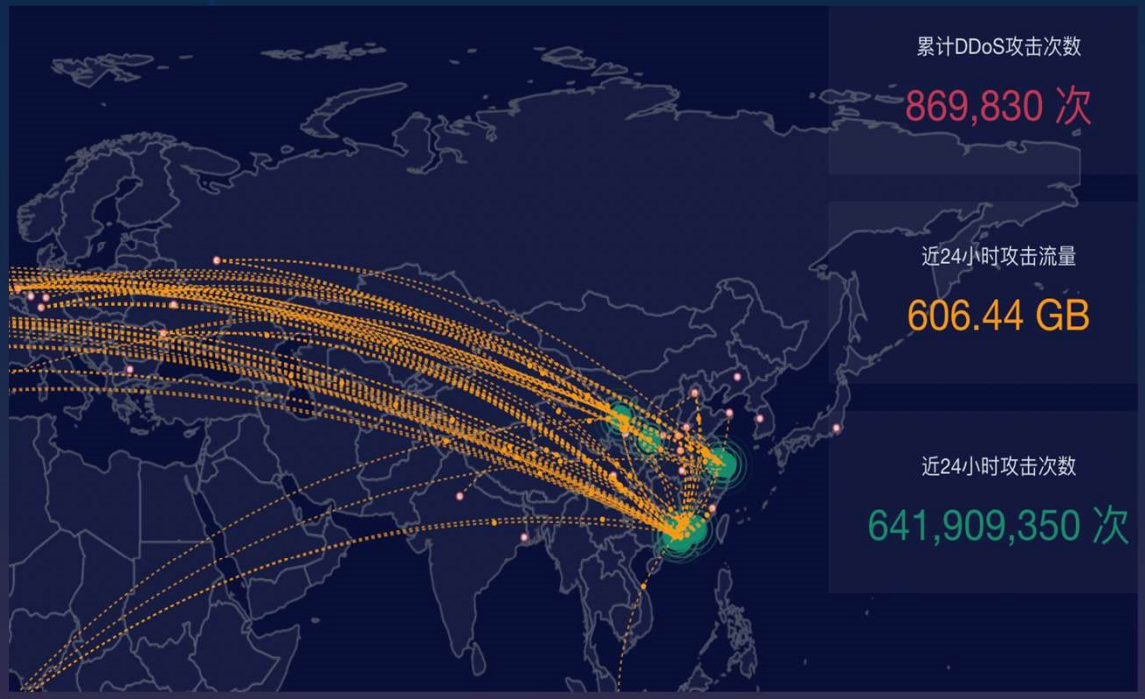
为了帮助业内更好地抵御基础CC攻击

百度安全计划开源Anti-CC脚本

防护DDoS/CC攻击的安全健壮基线

方向	防御点	说明
域名调度	DNS TTL	从600-->60,以支持快速解析变更与切换
	HTTPDNS	APP业务启用，秒级调度
	域名托管	选用具备DNS攻击防护能力的域名服务商
网络层	开启 Syn cookie	Linux服务内核开启Syn Cookie，缓解Syn flood攻击
	云上基础防御	利用好云平台提供的免费攻击防护能力
主机层	防火墙/安全组	做好必要的加固（端口/黑白IP限制等）
	AntiCC脚本	秒级拉黑僵尸IP，缓解服务资源占用
业务层	资源隔离	资源基于业务隔离（包括动静分离，前/后端拆分API）
	后端系统隐藏	避免后端业务对外直接暴露（如数据库等）
	建立攻击应急方案	如系统弹性扩容Auto Scaling、服务降级、关键业务必要时加入和开启人机识别（如验证码弹出）、关键业务静态维护页面等
完整防御	结合第三方商业化服务	接入第三方防攻击服务，完善整体防御预案

第三章 大流量下的攻击对抗

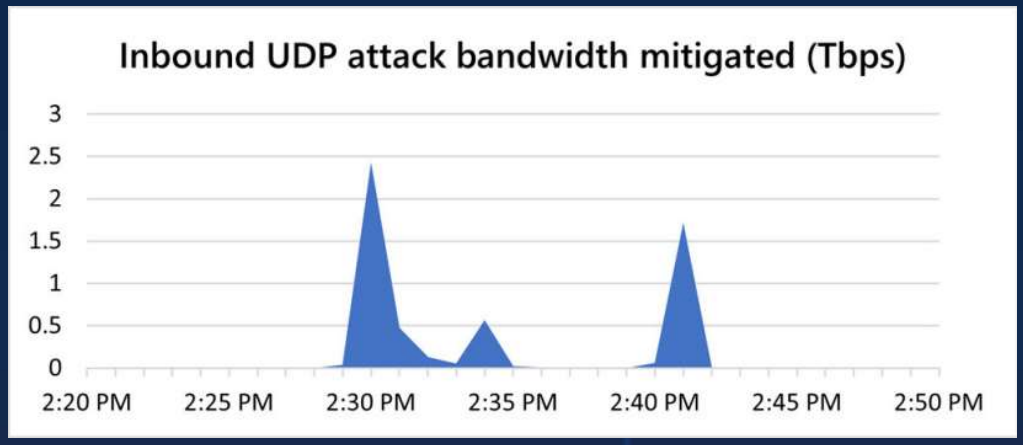


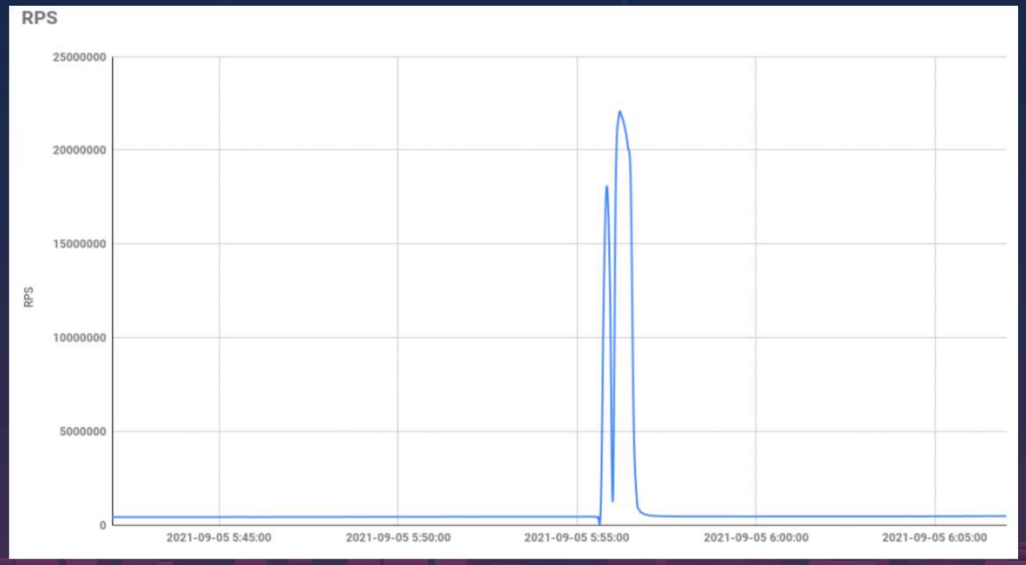
全网DDoS攻击年度峰值趋势

黑客掌握的资源越来越多

- 可反射的服务多
- 不安全的IOT设备多
- 有风险的移动APP多

史上最大的DDoS攻击





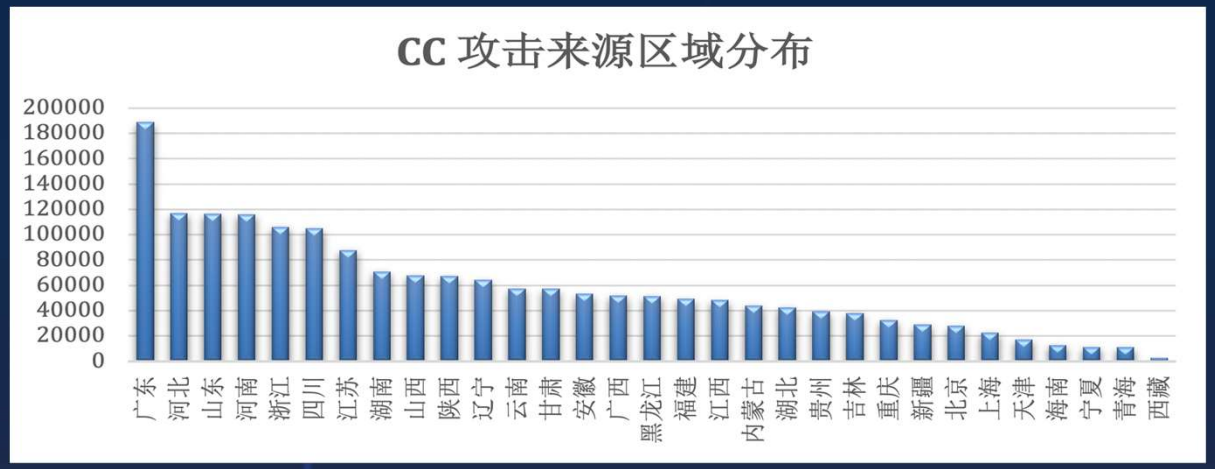
微软 Azure 2021年八月遭受到2.4 Tbps攻击

Yandex 2021年九月遭受到2180万RPS攻击

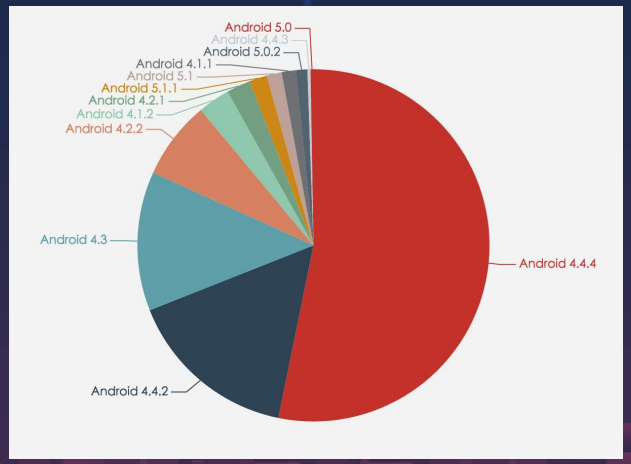
百度客户2017.02.23遭受到2000万RPS攻击
被成功防御

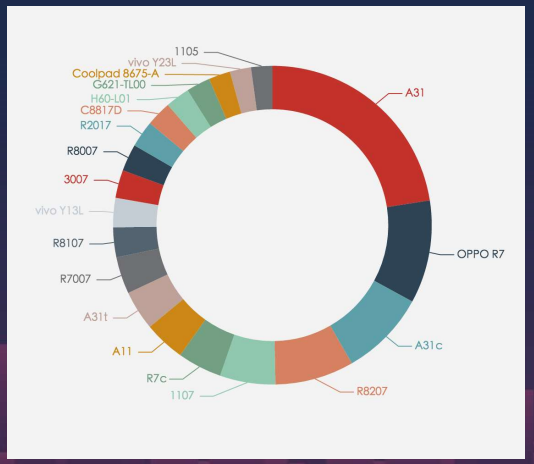
2000万RPS攻击

黑客团伙发起的攻击峰值超过2000万rps，真实IP源数量超过200万个，总流量达到100Gbps。



黑客通过恶意免流APK软件控制了手机僵尸网络

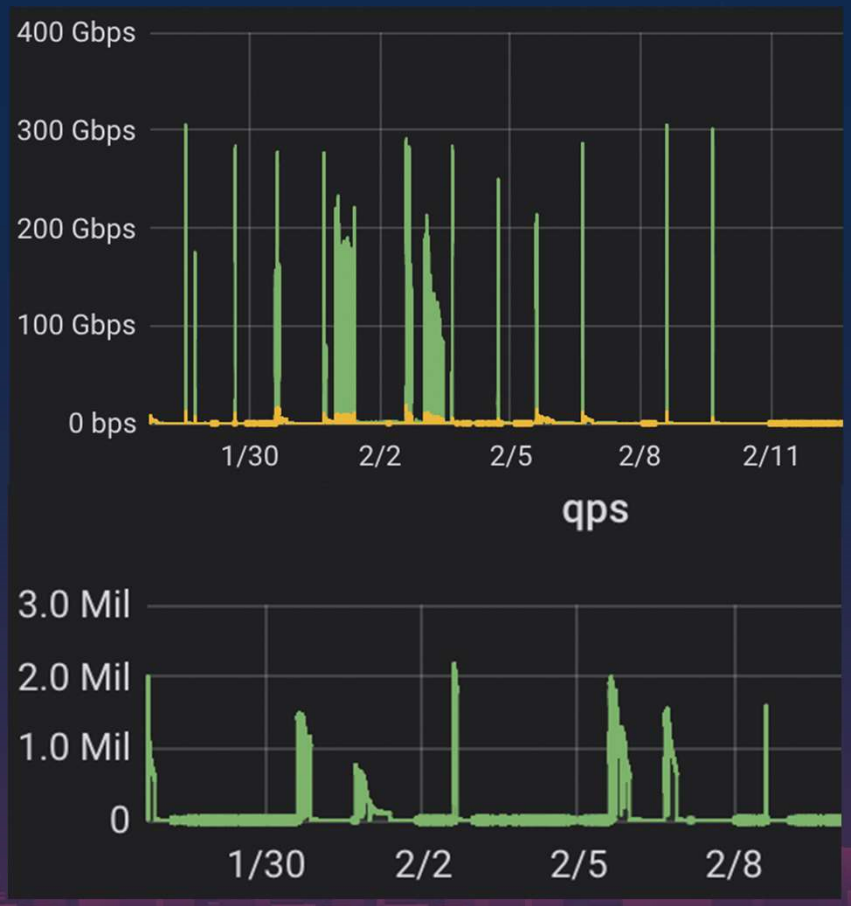




除了嵌入式设备，越来越多的手机设备，
逐渐在黑客攻击中崭露头角

对抗恶意僵尸网络

2021年1月10日-2月10日，一个客户连续遭受到1个月持续300G+ 流量攻击和200万RPS的CC攻击。



攻击特征：

\xB2\xBB\xCA\xCA\xD3\xC3UA GBK编码不适用UA

溯源分析，为恶意黑客组织七色光联盟---近期出现的互联网毒瘤。

已经锁定CC服务器，并提交给公安。

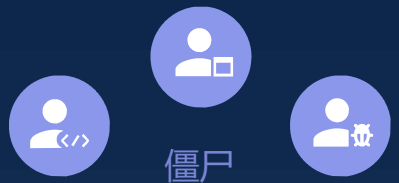
第四章 超大流量的防御体系

攻击对抗的本质：成本不平衡

DDOS解决方案

安全厂商云防御

100G保底
每天花费1万+



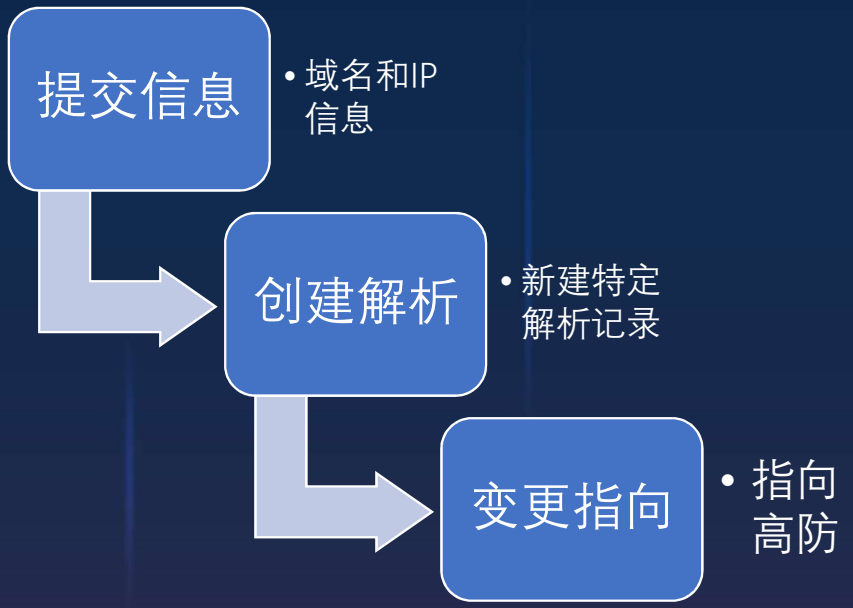
僵尸
网络

100G，花费成本<500

守护者计划

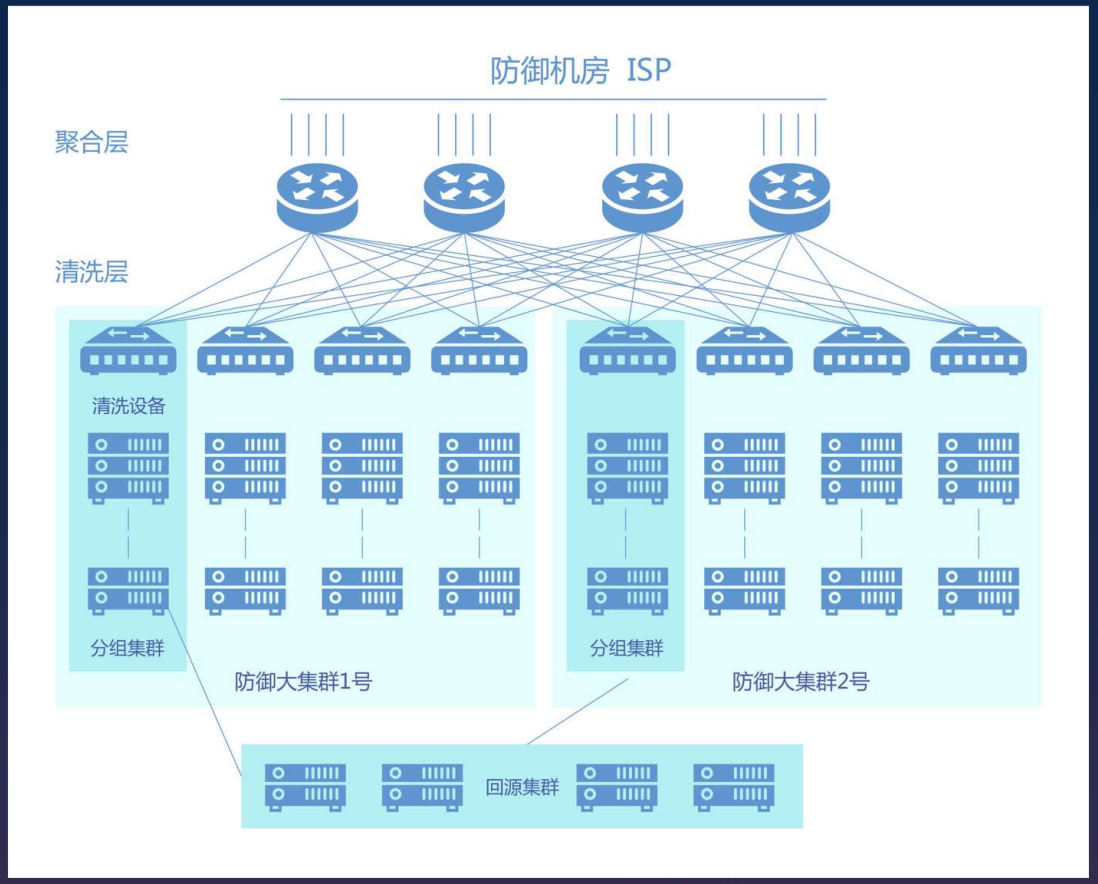
百度云高防推出守护者计划

净化网络，打击黑客组织嚣张气焰，帮助中小站长进行安全防护



三步接入法，CC防御无上限

超大攻击防护节点



百度云与安全团队自主研发倾力打造的超级抗D中心，为合作伙伴和客户提供安全防护，最大可防御 *Tb* 级攻击

防御线路

BGP（电信、联通、移动、30线+小运营商）

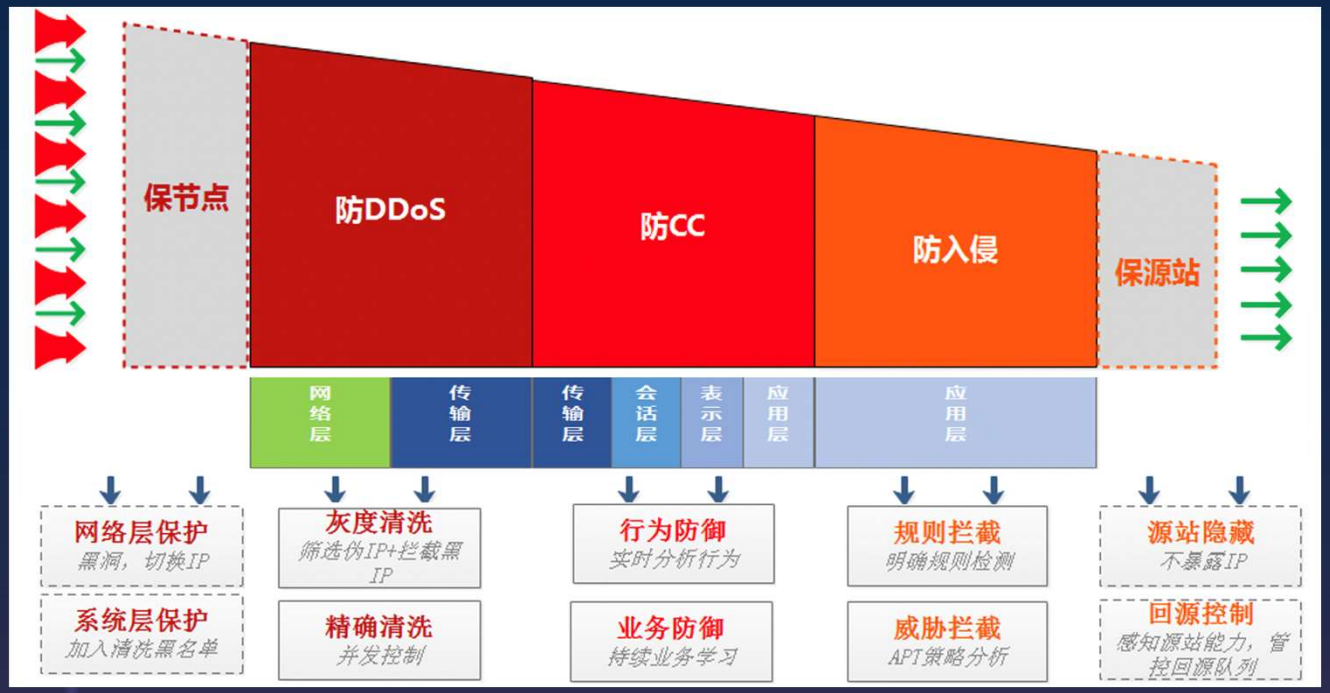
防护协议

Http、Https、TCP、UDP

回源方式

四层/七层反向代理

超大攻击防护模型



关键点：

- 分层防御
  - 三四层流量清洗
  - 五-七层CC防御
- 黑IP清洗
  - 多次攻击大搜的攻击源IP匹配达到80%+
- 行为防御
  - 访问集中度
  - 恶意特征
  - 异常访问比例
- 规则拦截
  - 自动提取恶意HOST特征
  - 指纹规则防御

百度安全简介


AI安全


移动安全


云安全


数据安全


业务安全

百度安全是百度公司旗下，以AI为核心、大数据为基础打造的安全品牌，是百度在互联网安全21年安全实践的总结与提炼。首创AI安全Security、Saftety、Privacy三大维度，研究方向涵盖AI安全、云安全、数据安全与隐私保护、物联网安全等前沿安全领域；业务覆盖百度各种复杂业务场景，同时面向安全生态、商业合作伙伴输出安全产品与行业一体化解决方案，全面护航AI时代云上安全各大业务场景。