字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY

第四期

字节跳动DDoS防护体系建设和实战

分享人：李明安

实战攻防

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

CONTENTS

实战攻防

Empower Security
Enrich life

01

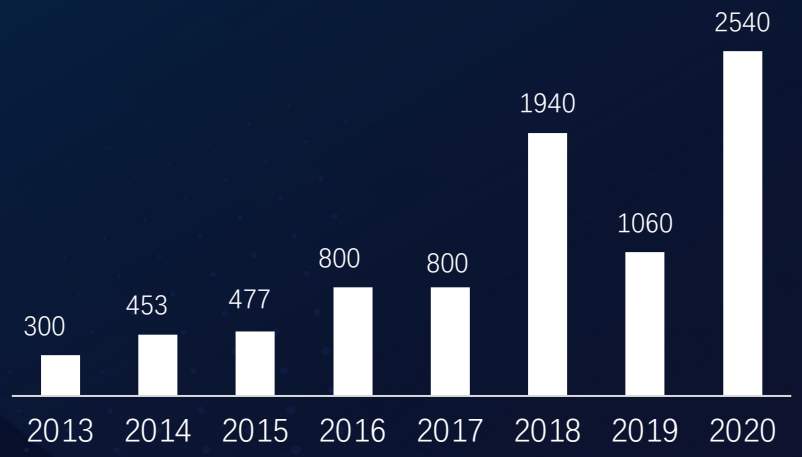
现网DDoS威胁态势

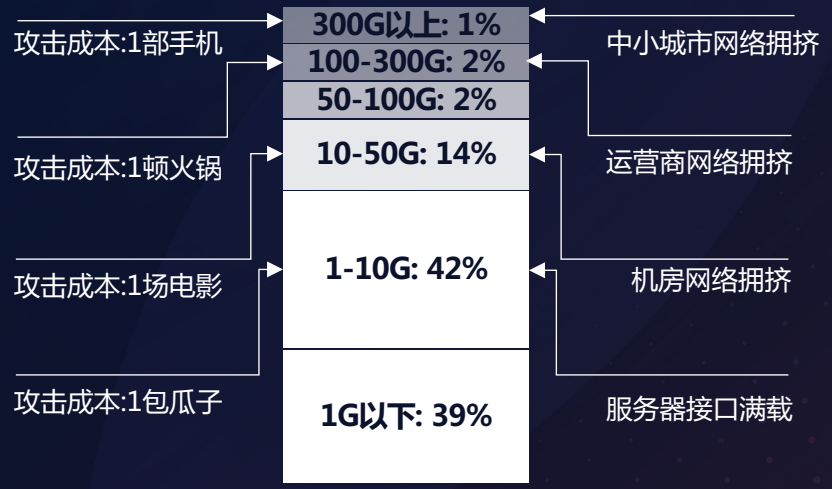
字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

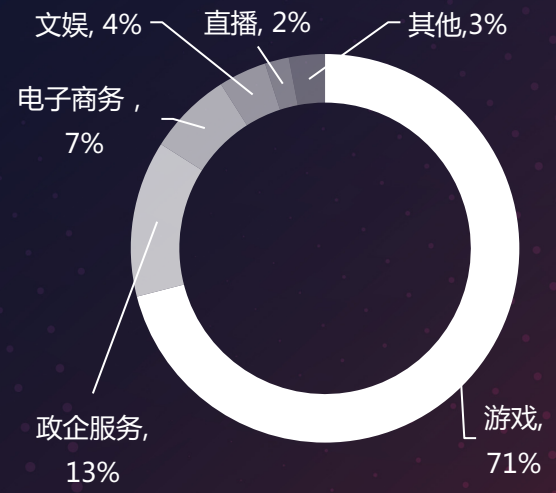
DDoS安全态势

- DDoS攻击从未停下增长的脚步

■ 业界攻击峰值







实战攻防

Empower Security
Enrich life

那问题来了

DDoS为何经久不衰，反而愈演愈烈

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

DDoS愈演愈烈的原因

天下熙熙，皆为利来；天下攘攘，皆为利往

- 成本低、防护难、溯源难、对黑客性价比高
- 黑客可通过勒索、恶意竞争等方式谋取暴利

性价比最高的武器


攻击成本低


防护难度大


溯源难度大


影响范围广

多种多样的获利方式


敲诈勒索


恶意竞争


恶意报复


游戏外挂变现

实战攻防

Empower Security
Enrich life

02

字节跳动DDoS防御体系

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

字节跳动DDoS防御体系

字节网络安全决策系统

配管 | 调度 | 计算 | AI

风控 | 情报 | 研究 | 主机 | 攻防 | 安全生态

端防护

水印

运营商防护

ISP黑洞

运营商ACL

近源清洗

运营商: 近源防御

云外高防

Anycast近源清洗

高防

流量调度

高防: 外边界防御

字节CDN

S-CDN抗D

CDN: 边缘防御

云

云DDoS

云FW

云 WAF

云NTA

云: 原生防御

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

字节跳动DDoS防御优势

海量防护资源

T级防护带宽， 有效应对大流量DDoS攻击带来的带宽资源压力

多层次防御体系

整合云原生防御、S-CDN、云外高防、运营商、端等多层次全链路覆盖的可靠防御体系

技术优势

字节跳动有优秀的AI算法实战经验积累，团队目前正在探索和搭建AI-DDoS防护体系，突破传统防护瓶颈

那问题又来了

DDoS就是简单粗暴打流量吗？ 防护难点在哪里

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

DDoS攻防正快速升级换代

攻

新型DDoS

TCP四层CC | UDP重放 | AI HTTP CC | 超大规模DDoS

.....

| 模拟业务 | 重放攻击 | 智能攻击 | 攻击流量上T

传统DDoS

SYNFLOOD | UDPFLOOD | .....

防

新一代DDoS防护

AI防护 | 流量指纹 | 双向流量识别 | Anycast近源清洗

传统DDoS防护

Syncookie算法 | UDP限速 | .....

实战攻防

Empower Security
Enrich life

03

现网DDoS对抗案例

网络勒索猖獗

- 由于巨大利益驱动，网络勒索的恶性事件不断增多，严重危害互联网安全

美国输油管道遭黑客攻击勒索

多个黑客组织向全球数千家互联网企业发起DDoS攻击威胁

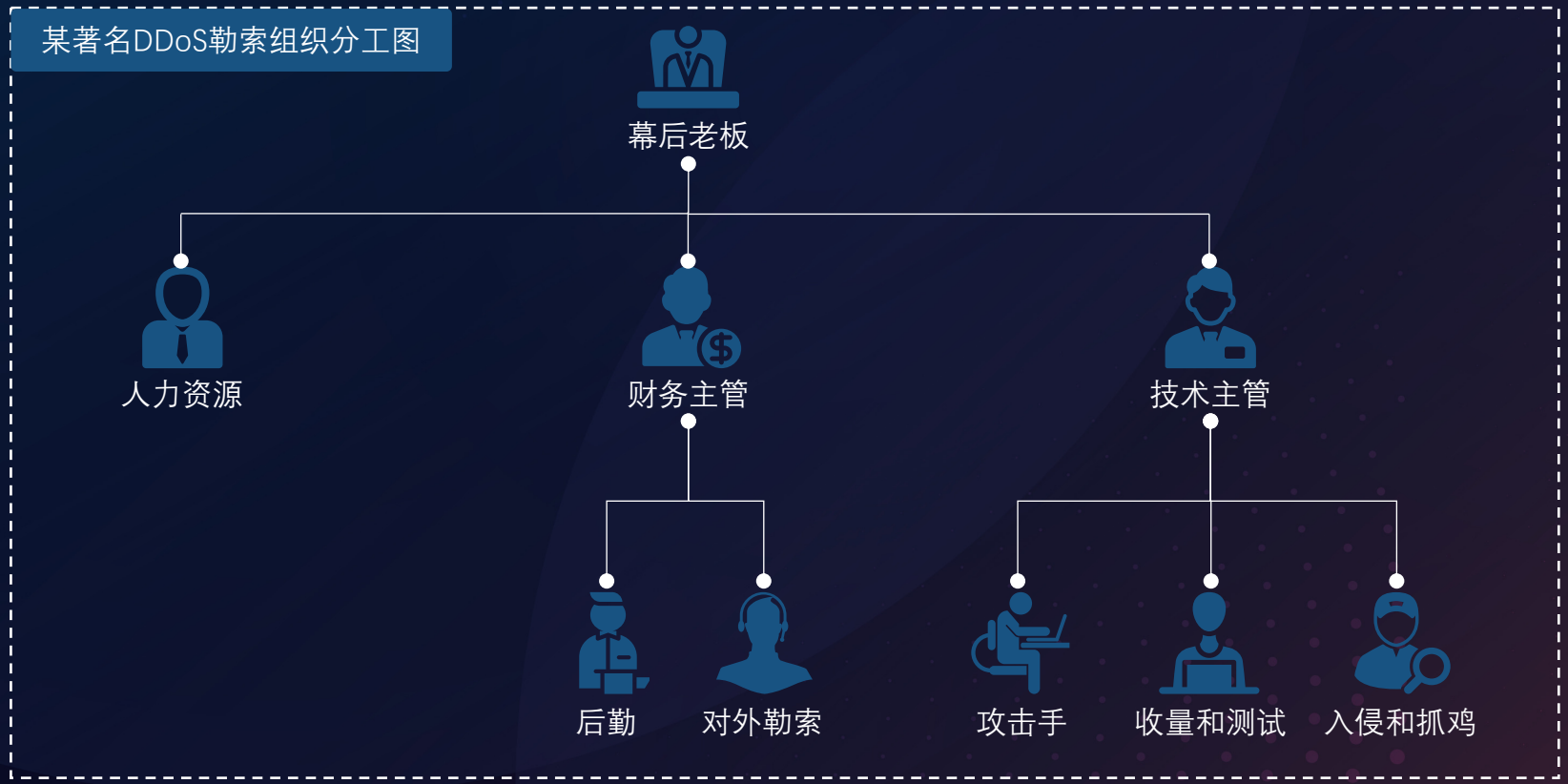
2020-10-18 19:31

近日，一批声称来自Armada Collective、Cozy Bear、Fancy Bear和Lazarus Group等黑客组织的攻击者们，对全球多个行业的数千家企业机构受到DDoS攻击威胁，向其勒索比特币。特别是亚太地区以及欧洲地区企业收到的勒索信日益增加。最开始遭到勒索威胁的一般都是金融服务业，但最近也开始将目标对准了其他行业机构，包括商业服务、高科技、酒店、零售和旅游等行业。

全球DDoS勒索事件日益增加

网络勒索产业链成熟

- 其实利用DDoS的网络勒索产业已经很成熟，早已形成组织有序、分工明确的团伙组织。是有组织有纪律的专业性产业。



字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

某公司海外机房遭受DDoS勒索

- 6月的某一天，端午节前夕，某公司机房遭受海外黑客组织勒索，要挟通过大规模DDoS，瘫痪其海外业务

We are the [redacted]s and we have chosen [redacted]s target for our next DDoS attack. Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days, on Tuesday next week. (This is not a hoax, and to prove it right now we will start a small attack on a few IPs from your [redacted]or actually just [redacted]) that will last for a couple of hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.)

There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps) This means that your websites and other connected services [redacted] will be unavailable for everyone.

We will refrain from attacking your network for a small fee. The current fee is 5 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide! We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 10 BTC and will increase by 5 Bitcoin for each day after the deadline that passed without payment. Please send Bitcoin to the following Bitcoin address: [redacted] Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do.

We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again. Please note we will respect your privacy and reputation, so no one will find out that you have complied.

黑客组织情报

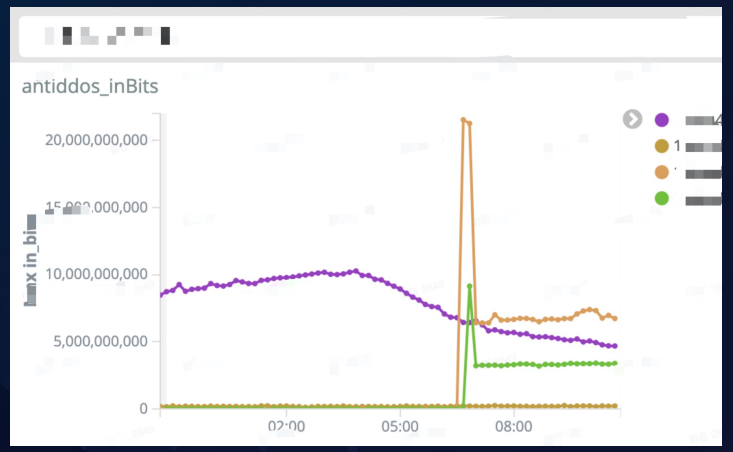
- “Fancy Lazarus”近期很活跃的DDoS勒索组织，在全球发起过多起勒索事件
- 2021年2月，新西兰的一些公司遭受“Fancy Lazarus”勒索，最大攻击流量236Gbps。
- 2021年5月，多个组织报告称，一个所谓"Fancy Lazarus"的组织发了多起DDoS勒索活动
- 2021年6月，来自不同网络安全公司和网站的多份报告警告说："Fancy Lazarus"又开始了网络攻击。

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

发起勒索的同时，黑客先打几波DDoS以作警告

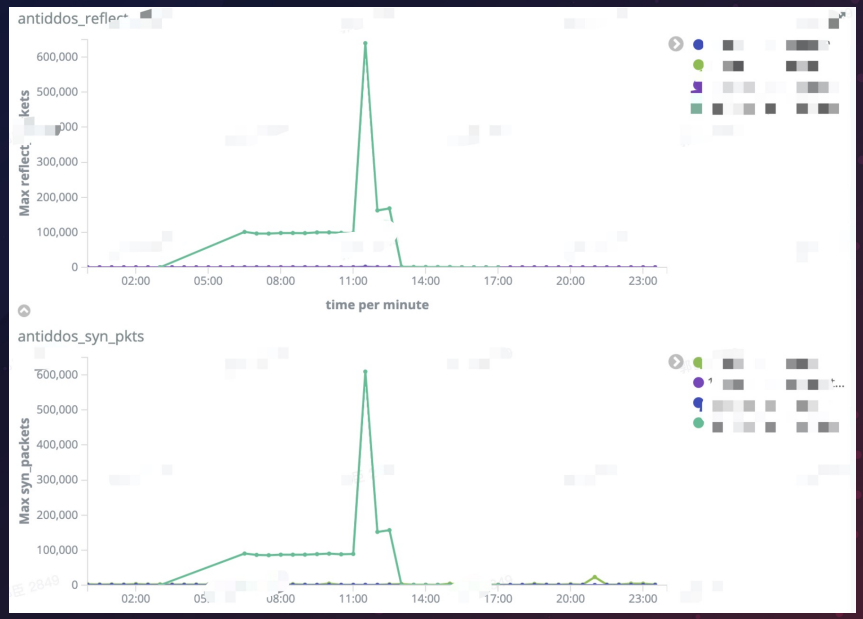
- 在收到邮件的同时，黑客还对目标机房3个IP发起DDoS攻击，以作警告。
- 3个IP遭受持续七个半小时的DDoS攻击，单dstip峰值21.5G，手法包括UDPFLOOD和SYNFLOOD。

IP 1：DDoS态势



IP 2： DDoS态势

IP 3： DDoS态势



实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

那问题又又来了

面对来势汹汹的DDoS勒索，应该如何应对

实战攻防

Empower Security
Enrich life

事前、事中、事后的一体防御体系

- 为有效解决DDoS勒索，保障业务稳定，安全团队牵头搭建一套完备的防御体系

事前

- 情报收集
- 业务信息收集
- 权威DNS加固
- IP网段备用
- 攻击演练
- 防护方案梳理
- 应急预案

事中

- 流量监控
- 自动告警
- 7*24值守
- 字节DDoS防护
- 运营商防护
- 第三方高防

事后

- 攻击溯源
- 联系监管部门
- 复盘和总结

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

事前：知己知彼 百战不殆

- 不打无准备之仗

实战攻防

Empower Security
Enrich life

事中：整合力量 联合作战

- 该公司安全团队整合自研DDoS系统、ISP清洗能力、第三方高防厂商能力，搭建多层防御体系

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

多轮DDoS轰炸被成功防护

- 第一轮：6月14日 黑客声称的攻击日期 ，攻击如期而至，机房遭受大规模DDoS攻击。

6月14日DDoS攻击，峰值141G，但被精确识别和清洗，业务没有被影响

实战攻防

Empower Security
Enrich life

字节跳动 安全中心 × 安全范化 BYTEDANCE SECURITY

多轮DDoS轰炸被成功防护

- 第二、第三轮：黑客仍未放弃，在6月16日继续对机房其他IP发起2次 DDoS，攻击流量峰值14Gbps。但攻击再次被成功防护，黑客最终放弃攻击。
- 经过分析，这些攻击在手法、来源IP归属、端口、流量特征等维度都有很强的相似性，故基本确认就是同一个黑客团伙所为

攻击手法

攻击手法上都是以UDP为主夹杂其他流量的混合型DDoS

来源IP归属

来源IP在地理位置归属、ISP归属上存在很高的吻合度

多次攻击对比分析

攻击端口

攻击端口都是业务端口，都是非常具有针对性

流量特征

攻击流量在载荷、包长等特征维度上均有很高的吻合度

事后：攻击溯源 复盘沉淀

- 成功防护DDoS不意味着事情的结束，还需做攻击溯源等分析工作，更重要的是复盘和总结，不断提升团队战斗力

攻击溯源

分析攻击来源、攻击手法、流量特征等数据，并结合威胁情报、网络情报、反向跟踪分析等手段对攻击者进行溯源

联系监管部门

联系当地网络安全监管部门，如US CERT，寻求国家安全部门、运营商的帮助

复盘和总结

对整个事件的响应和处理方案进行了深刻的复盘和总结，通过复盘和沉淀进一步提升团队对抗DDoS的响应效率和战斗力

字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY

THANK YOU