



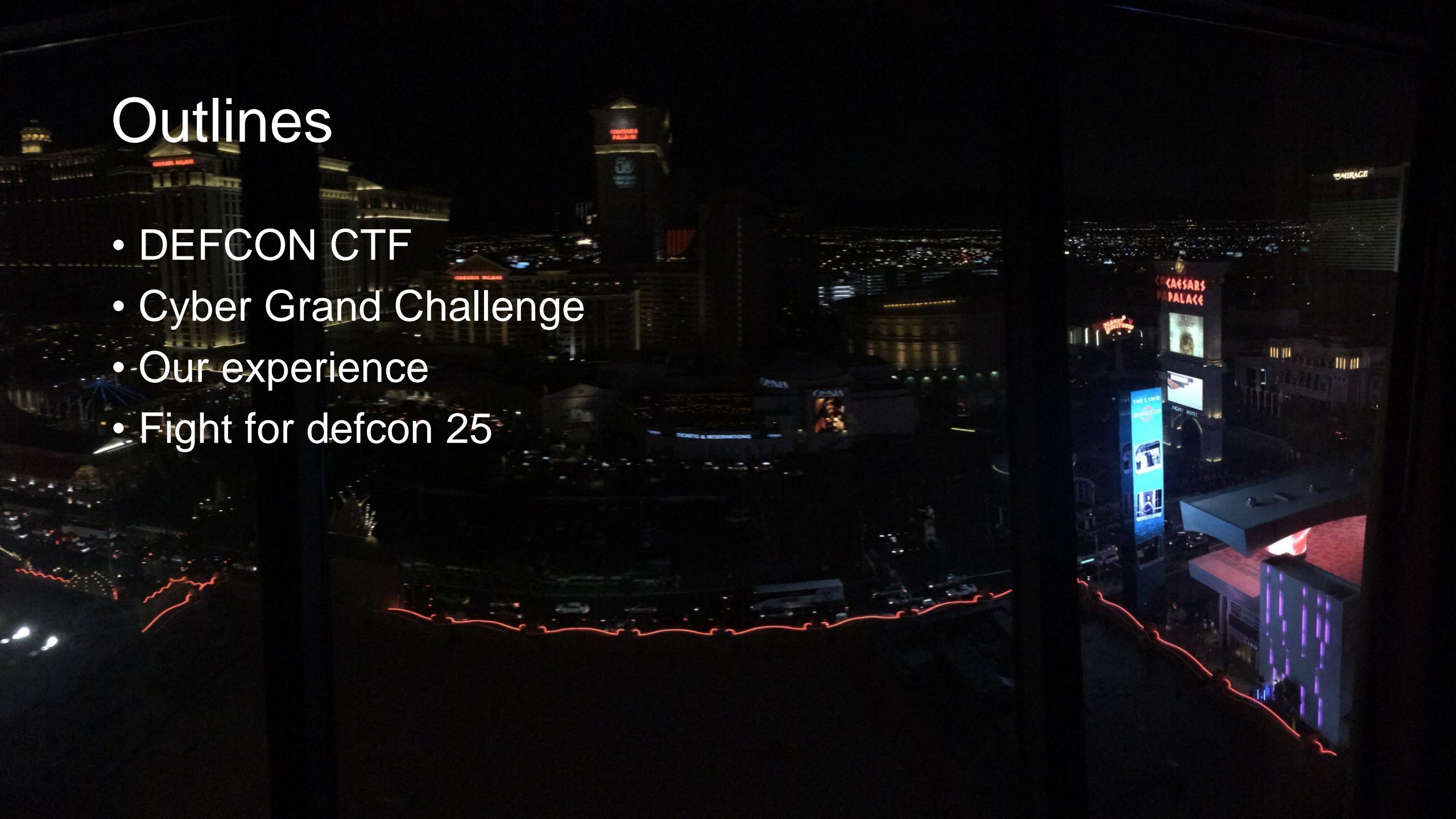
# DEFCON 24 决赛介绍

BrieflyX 裴中煜



# Outlines

- DEFCON CTF
- Cyber Grand Challenge
- Our experience
- Fight for defcon 25





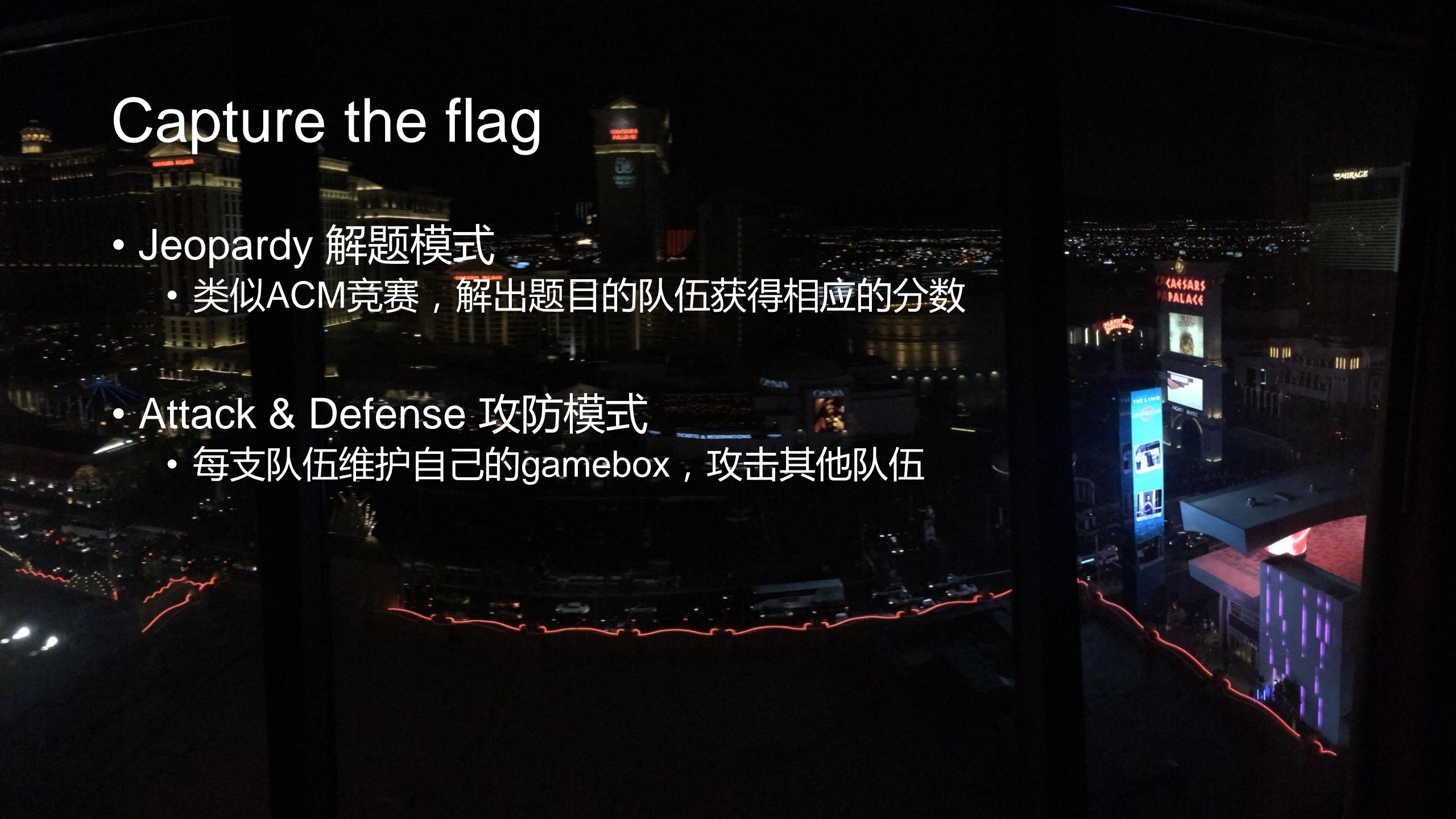
# Capture the flag

- 黑客之间的较量
- 领域涵盖逆向分析、Web渗透、漏洞利用、流量分析、电子取证.....
- 以夺得旗帜（flag）为得分标志



# Capture the flag

- Jeopardy 解题模式
  - 类似ACM竞赛，解出题目的队伍获得相应的分数
- Attack & Defense 攻防模式
  - 每支队伍维护自己的gamebox，攻击其他队伍





# DEFCON CTF

- 全球最著名的CTF比赛
- CTF界的“世界杯”
- 每年7-8月在拉斯维加斯举行





# DEFCON CTF

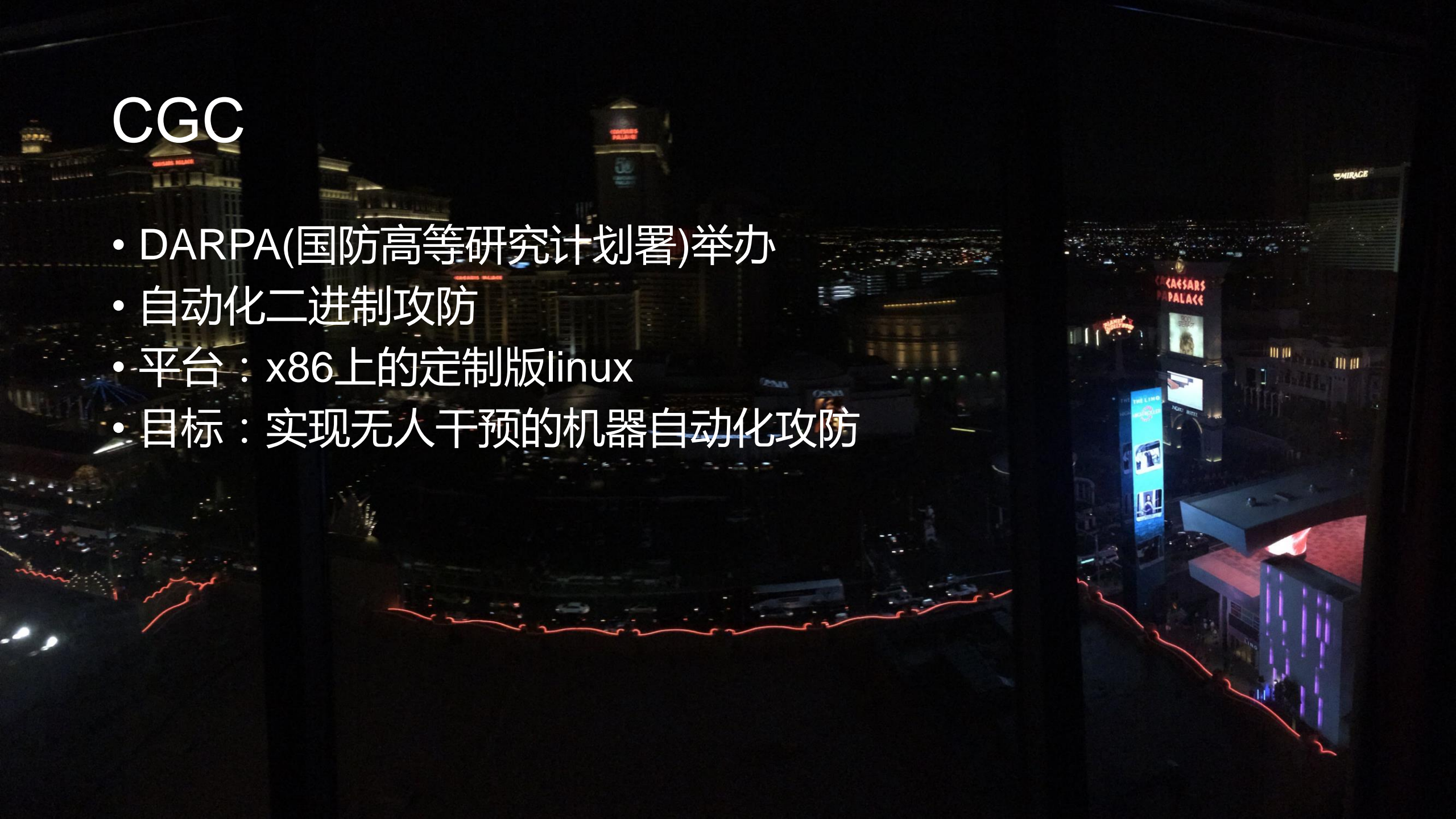
- 传统的Attack & Defense模式
- 多种架构：x86，arm，mips ...
- Defcon 24：采用Cyber Grand Challenge赛制





# CGC

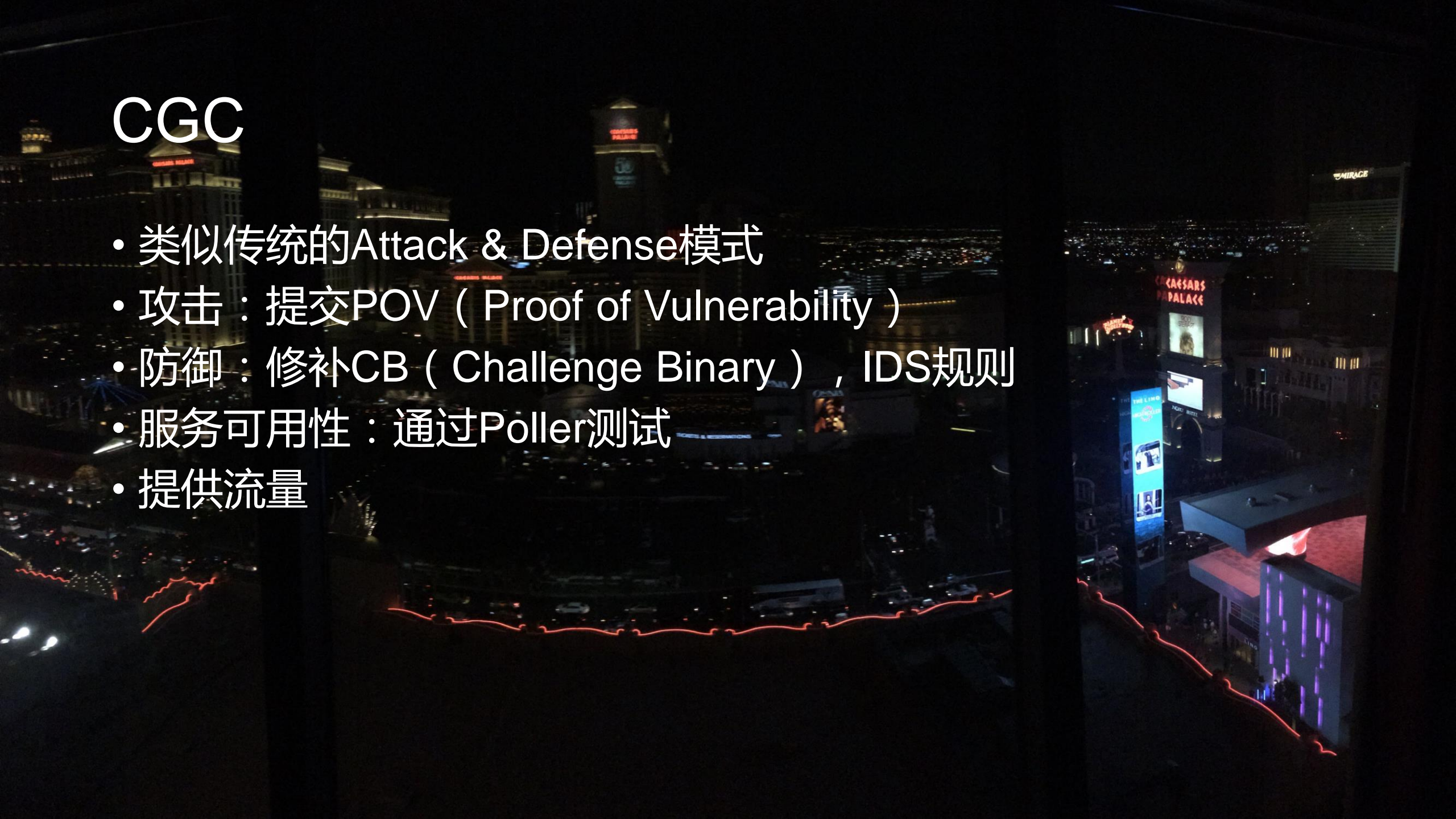
- DARPA(国防高等研究计划署)举办
- 自动化二进制攻防
- 平台：x86上的定制版linux
- 目标：实现无人干预的机器自动化攻防





# CGC

- 类似传统的Attack & Defense模式
- 攻击：提交POV ( Proof of Vulnerability )
- 防御：修补CB ( Challenge Binary ) , IDS规则
- 服务可用性：通过Poller测试
- 提供流量





# CGC

- 攻击成功的标志
  - Type I : 控制EIP与任意一个通用寄存器的20bit
  - Type II : 从指定的flag page (0x4347c000) 读出任意4个字节
- CB与IDS所有人可见



# CGC & Defcon

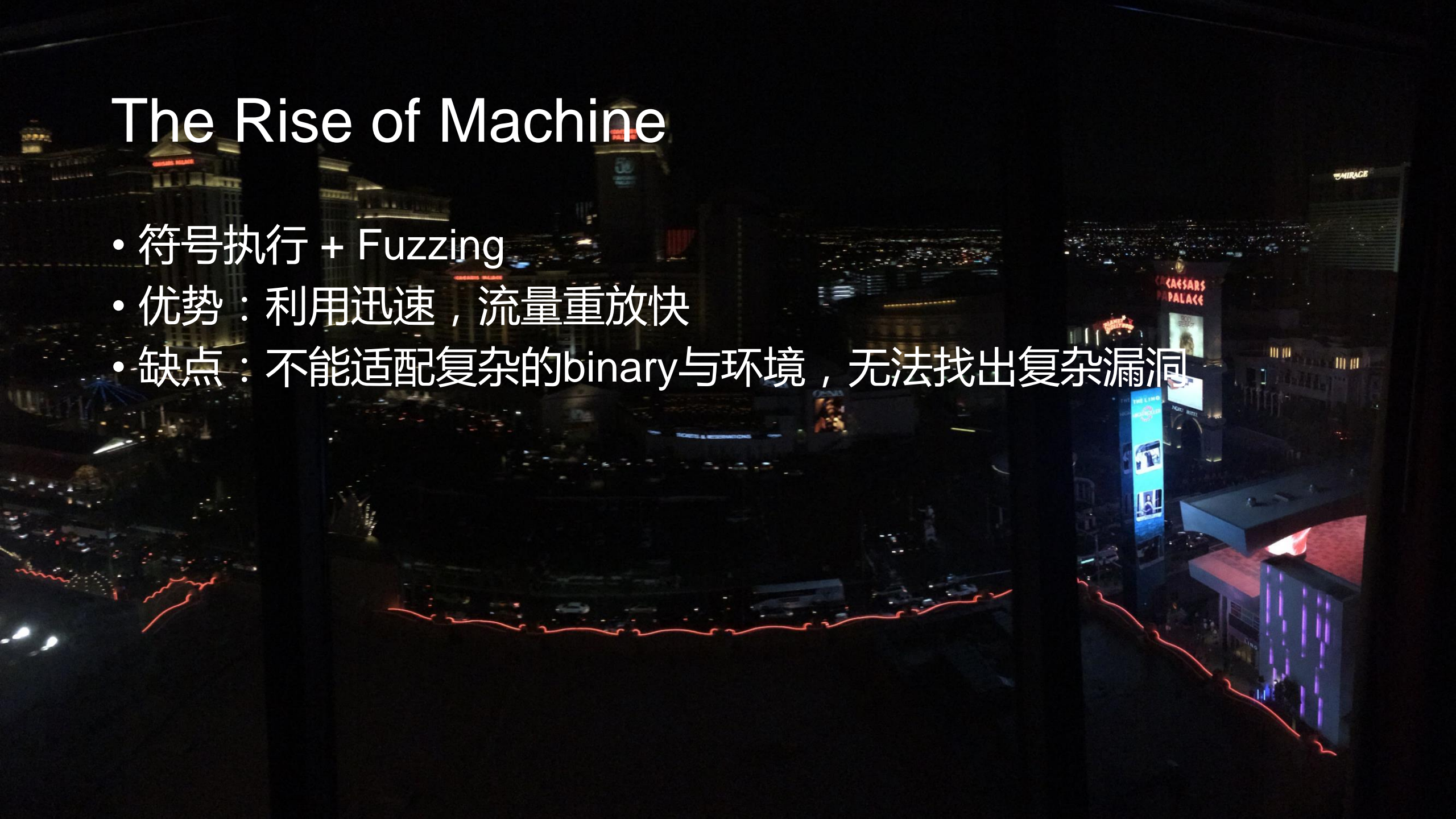
- 前一天举行CGC的决赛（ CGC Final Event, CFE ），决出第1名的机器队伍
- 在之后的Defcon CTF中，机器将与人同台竞技





# The Rise of Machine

- 符号执行 + Fuzzing
- 优势：利用迅速，流量重放快
- 缺点：不能适配复杂的binary与环境，无法找出复杂漏洞





# CFE





# Winner of CFE

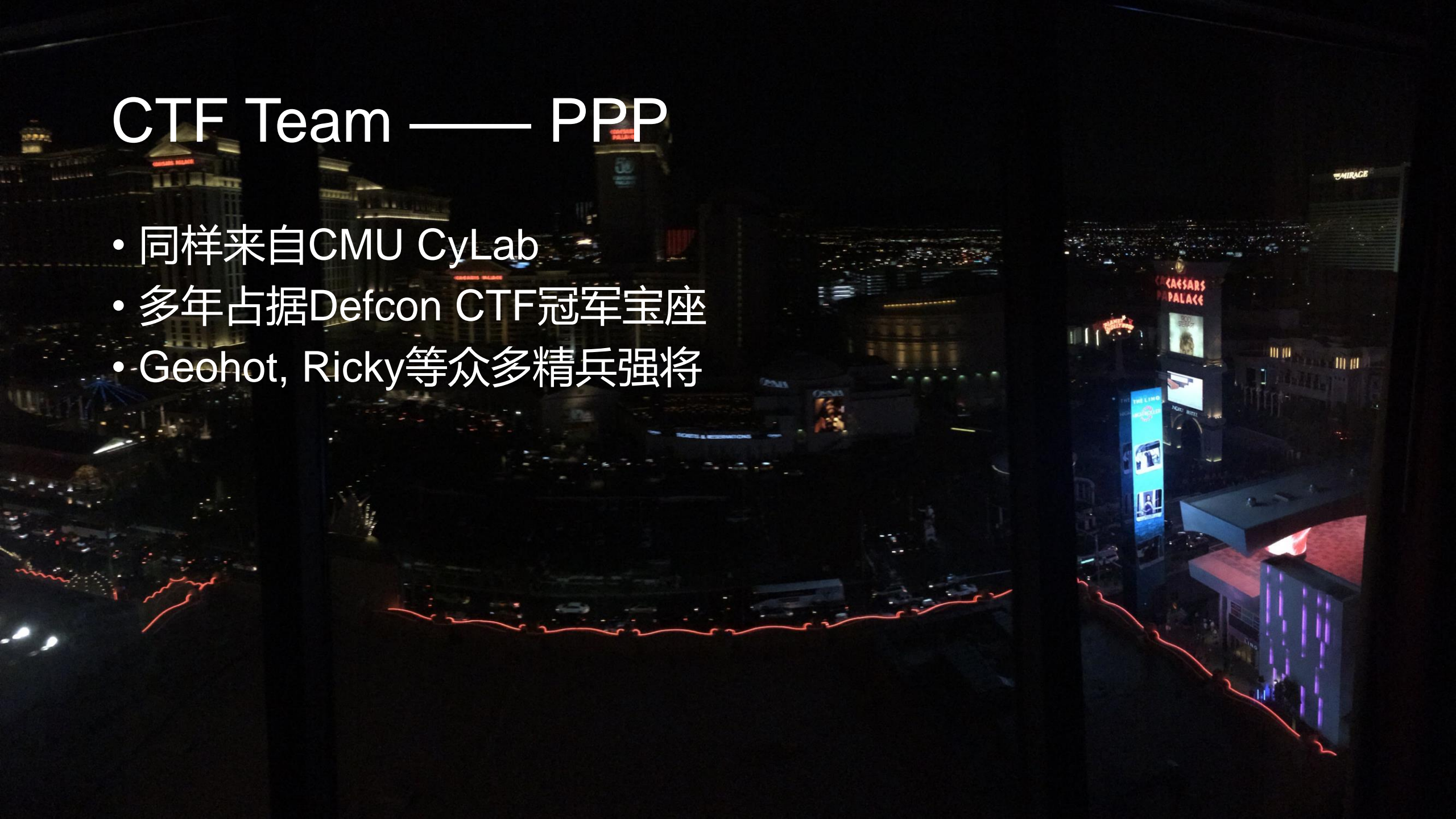
- ForAllSecure —— Mayhem
  - CMU教授David Brumley创立
  - 成员大多来自CyLab





# CTF Team —— PPP

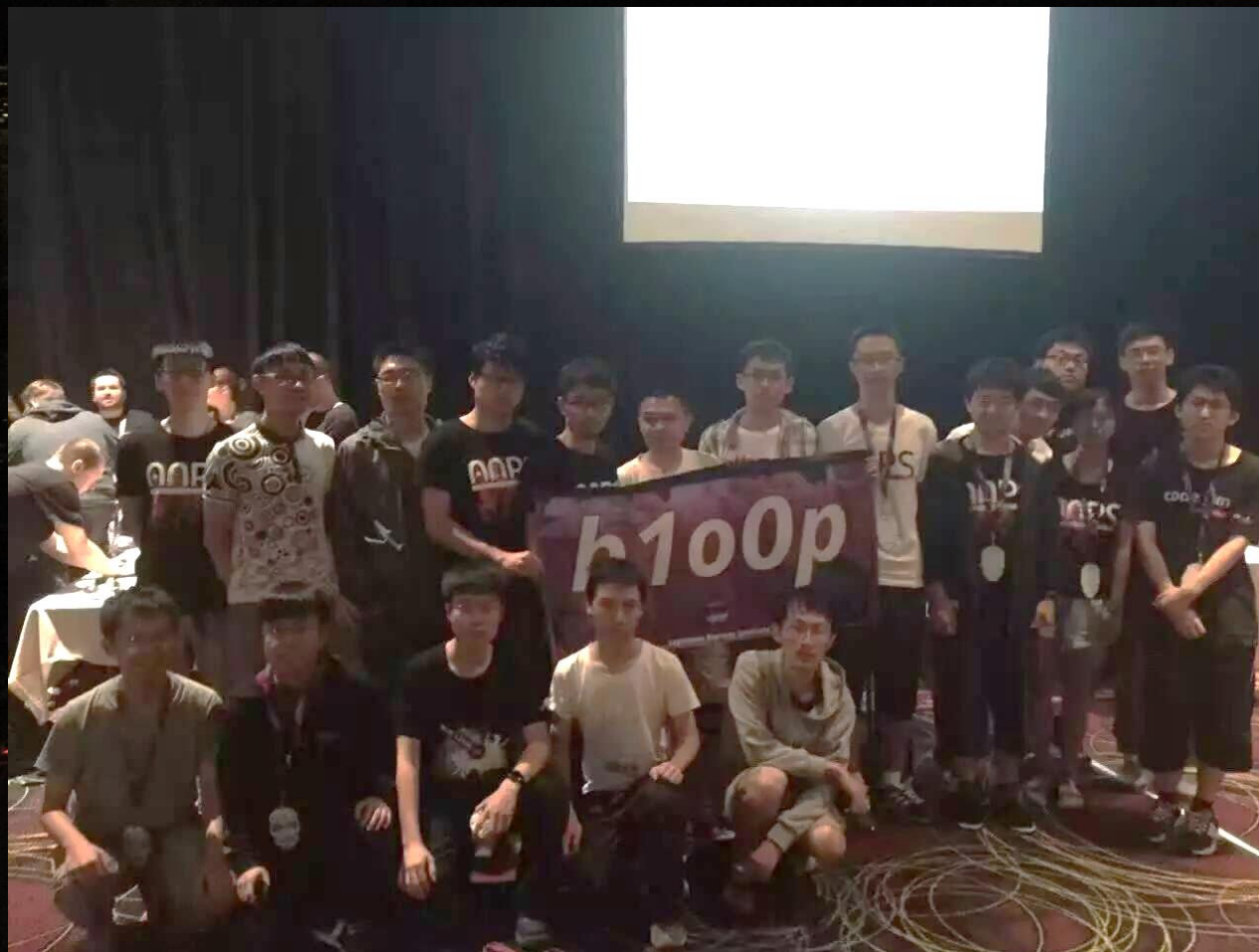
- 同样来自CMU CyLab
- 多年占据Defcon CTF冠军宝座
- Geohot, Ricky等众多精兵强将





# Our team — b1o0p

- Blue-lotus + 0ops





# Game arena





# Game arena II





# CTF Schedule

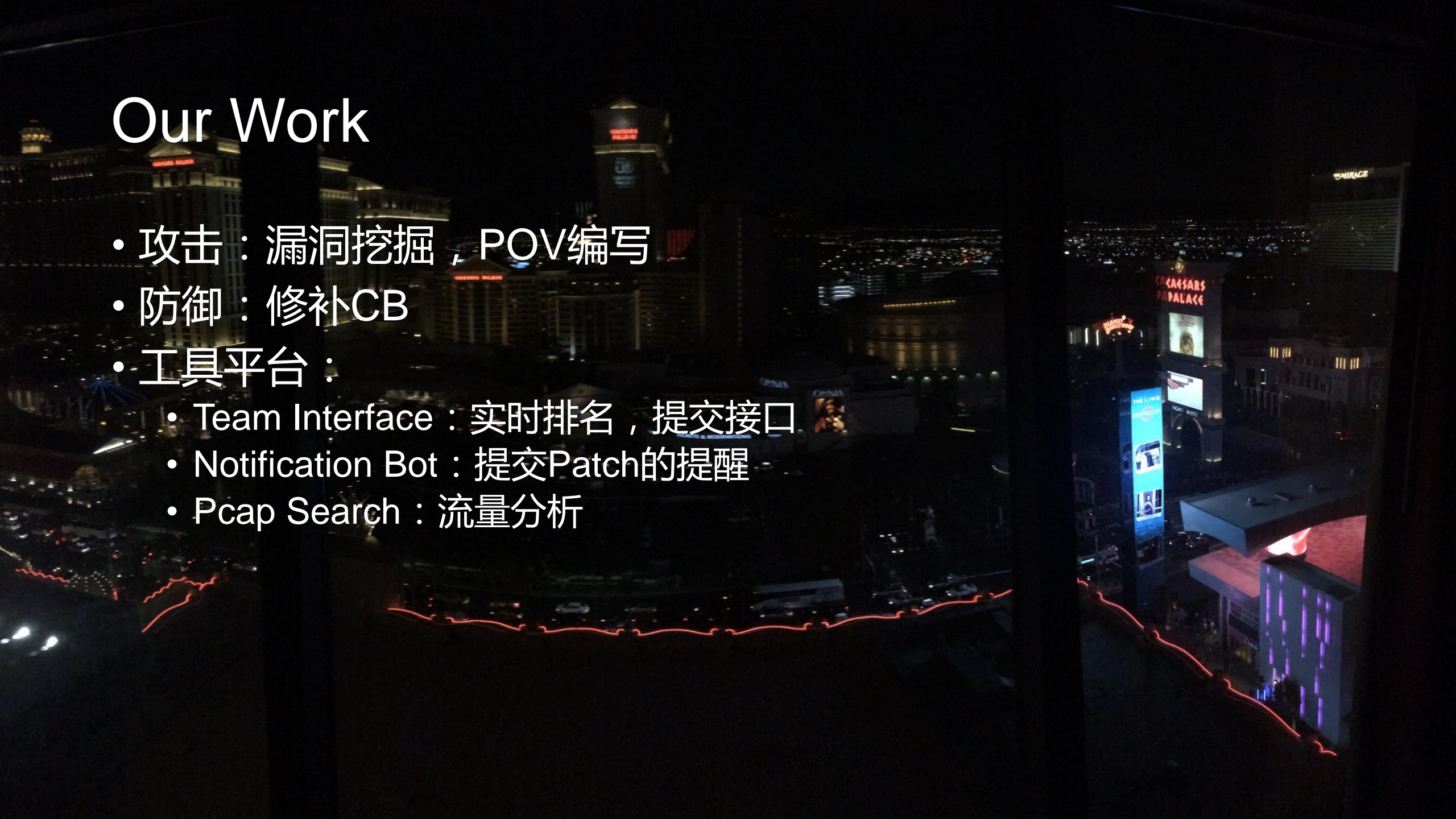
- 赛程一共3天
- 第2天时隐藏分数
- 第3天时隐藏排名





# Our Work

- 攻击：漏洞挖掘，POV编写
- 防御：修补CB
- 工具平台：
  - Team Interface：实时排名，提交接口
  - Notification Bot：提交Patch的提醒
  - Pcap Search：流量分析





# Team Interface

Defcon 2016 Admin Panel Round:163

Scoreboard

Dashboard


Submission <


Feedback information <


Consensus evaluation <


Notify <

## Scoreboard

163  
Round

2  
Rank

14  
Score

1  
Prev Team Score Diff

Search:

Rank	Team Name	Score	Last Round	Change Rank	Trend
1	PPP	15	0	1	0
2	b10op	14	0	1	0
3	DEFKOR	13	0	1	0



# First Day

- 接口调整，开始很晚
- 结束时位列第5

## Scoreboard

place	score	team
1	30214	DEFKOR
2	24220	PPP
3	22012	HITCON
4	21524	LC&BC
5	21282	b1o0p
6	21178	KaisHack
7		GoN



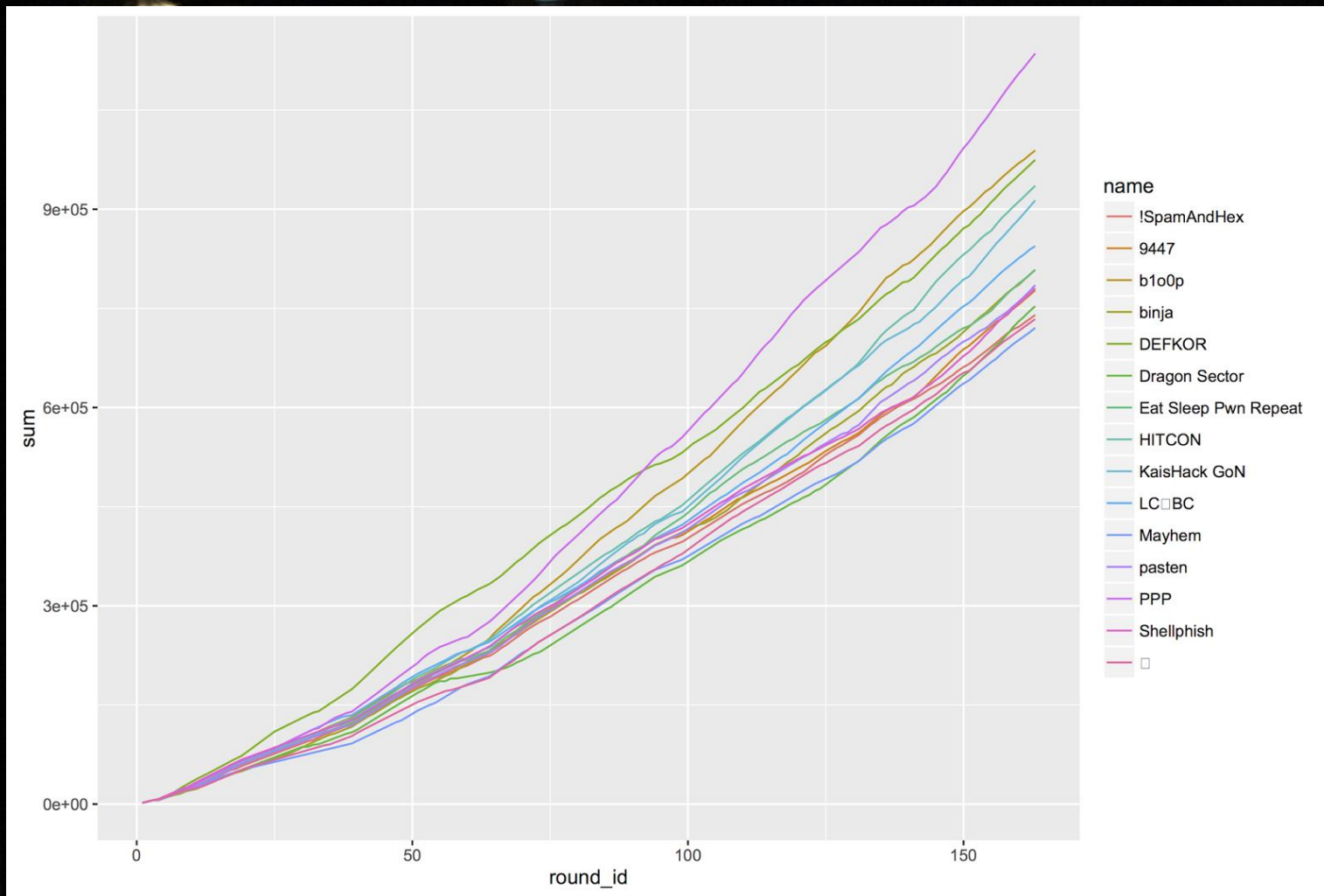
# Second Day

- PPP超越DEFDOR
- 结束时位列第2





# Final Result





# Final Result

- Second place
- 与PPP分差较大

Team	Final Score
PPP	113555
bloOp	98891
DEFKOR	97468
HITCON	93539



# Machine Behaviour

- Last place
- 平台略有不同，导致其流量分析重放无法工作
- 号称8个题目解出7题

Dragon Sector

75320

!SpamAndHex

73993

侍

73368

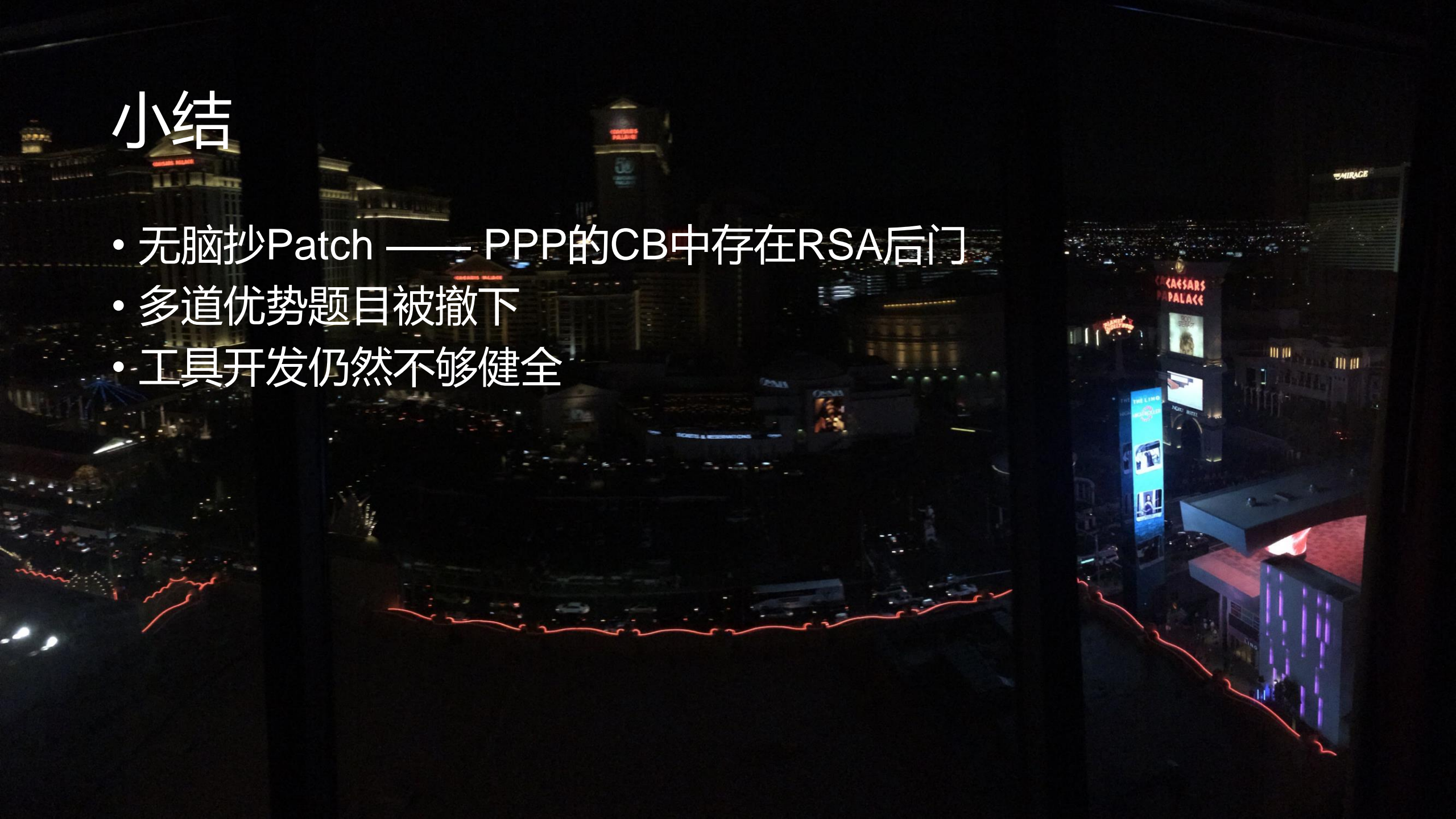
Mayhem

72047



# 小结

- 无脑抄Patch —— PPP的CB中存在RSA后门
- 多道优势题目被撤下
- 工具开发仍然不够健全





# This Year

## LIVE IN CONCERT

July 28-30, 2017

DEF CON 25

Caesars Palace, Las Vegas

Contest	Qualifying Team
<u>DEF CON CTF</u>	PPP
<u>RuCTFE</u>	Eat Sleep Pwn Repeat
<u>HITCON CTF</u>	Cykorkinesis
<u>33C3 CTF</u>	pasten
<u>Boston Key Party</u>	HITCON
<u>UCSB iCTF</u>	Bushwhackers
<u>0ctf</u>	TBA June 4, 2017
<u>PlaidCTF</u>	Tea Deliverers
<u>DEF CON CTF Qualifiers</u>	Shellphish
<u>DEF CON CTF Qualifiers</u>	A*0*E
<u>DEF CON CTF Qualifiers</u>	hacking4danbi
<u>DEF CON CTF Qualifiers</u>	!SpamAndHex
<u>DEF CON CTF Qualifiers</u>	RRR
<u>DEF CON CTF Qualifiers</u>	Team Rocket 🦋
<u>DEF CON CTF Qualifiers</u>	Lab RATs





THANKS