



清華大學

Tsinghua University

欲速则不达 CDN DDoS大炮

李伟中 沈凯文 郑晓峰 郭润 王垚 王郁 陈夏润

团队介绍

Team introduction

清华大学-奇安信集团网络安全联合研究中心



清华大学网络研究院和奇安信集团共同成立，团队在漏洞挖掘与攻防领域有丰富的经验，在国际四大顶级安全会议中发表多篇论文，在世界学术和工业界有广泛的影响力，孕育了“蓝莲花”等国际知名黑客战队。

清华大学网络与信息安全实验室（NISL）

段海新 诸葛建伟 张超



关于我

About me



沈凯文

清华大学网络安全实验室

导师：段海新教授 硕士在读

CTF：蓝莲花、Tea Deliverers战队成员

研究兴趣：协议漏洞挖掘、APT攻防对抗、机器学习
流量分析



CDN DDoS 大炮

CDN DDoS

项目概要：

1. 攻击者可利用CDN通用实现缺陷对任意部署Web服务的站点进行DDoS攻击；
2. 攻击者无需控制僵尸网络，仅通过较低配置的个人电脑、低带宽网络就可以发起大规模DDoS攻击，使对应的网站拒绝服务。

影响范围

1. 截至当前，已发现多个严重的通用缺陷；
2. 几乎所有主流CDN都可被用于实施DDoS攻击；
3. 所有网站都可能遭受攻击，部分CDN可能遭受攻击。

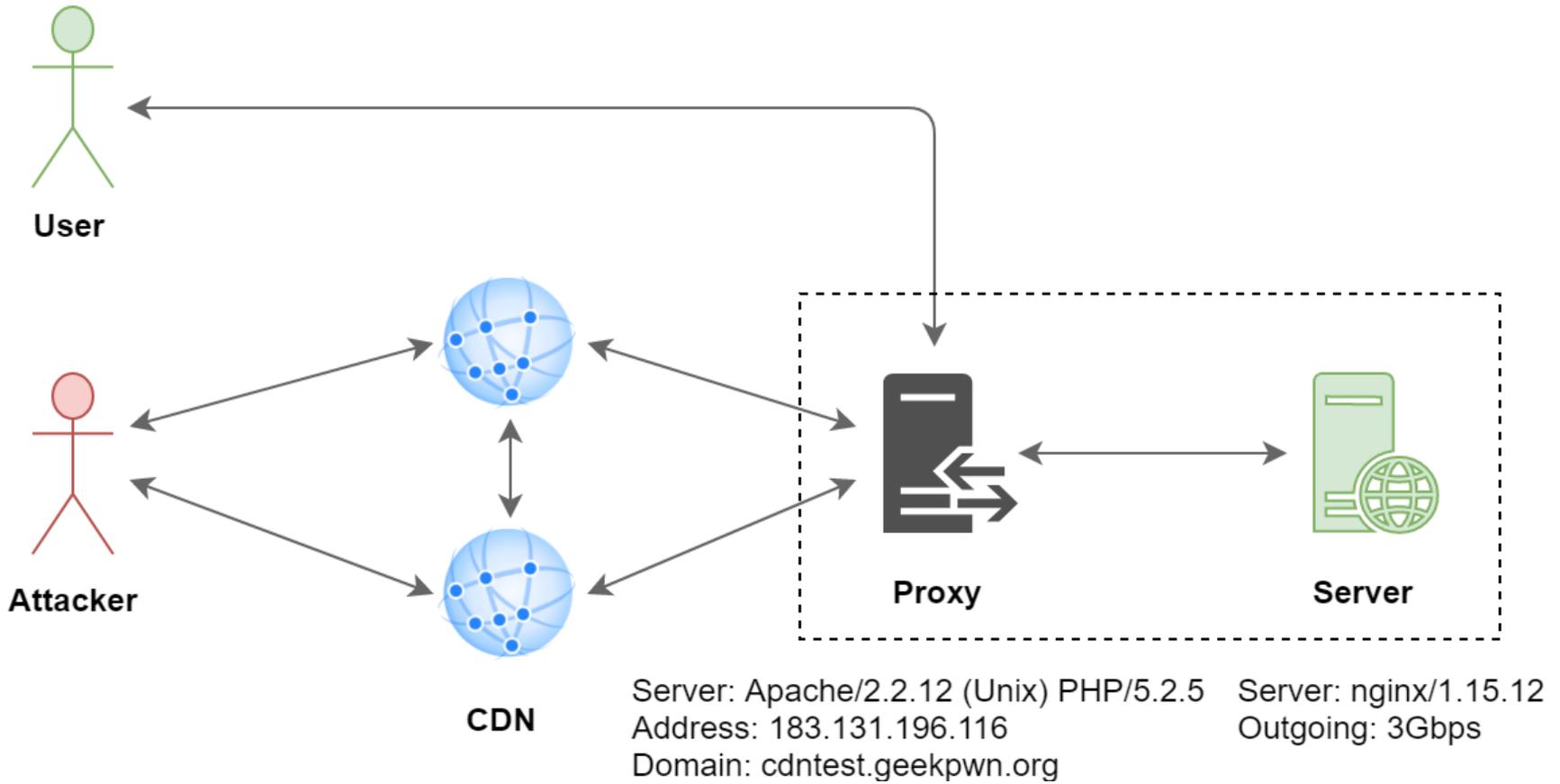
GeekPwn 现场

CDN DDoS



GeekPwn 攻击环境

CDN DDoS



一种新型的DDoS攻击

A new type of DDoS attack

1. 攻击者**无需控制僵尸网络**，仅通过**较低配置**的个人电脑、**低带宽网络**就可以发起**大规模DDoS攻击**；
2. 利用**CDN节点**进行**分布式回源**，传统DDoS防御方案几乎**失效**，且攻击者**难以被溯源**；
3. 与传统DDoS不同，该攻击主要攻击受害者的**出口带宽（主）、连接数（辅）**；
4. 该攻击可通过一定配置，**直接攻击CDN内部节点**，造成**CDN拒绝服务**。

GeekPwn 演示效果

CDN DDoS

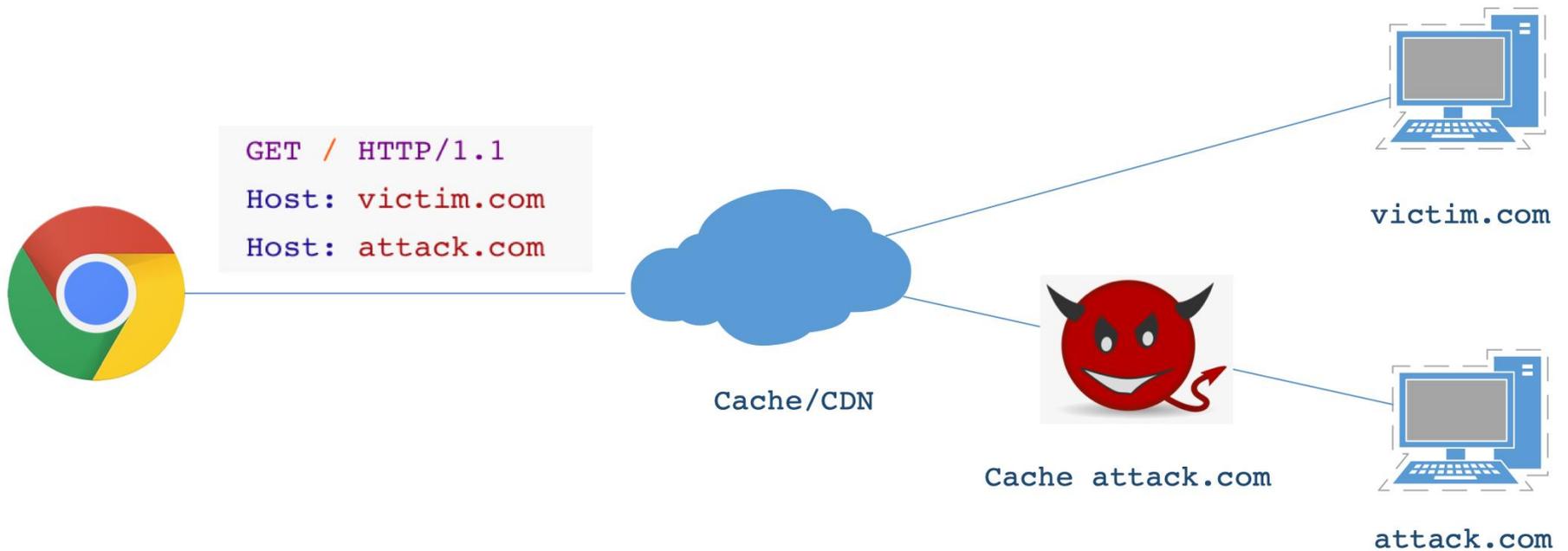


访问延迟(文件大小5MB): 2~3s → 20~30s

我们是如何发现此类攻击

How did we discover such attacks

协议不一致性：



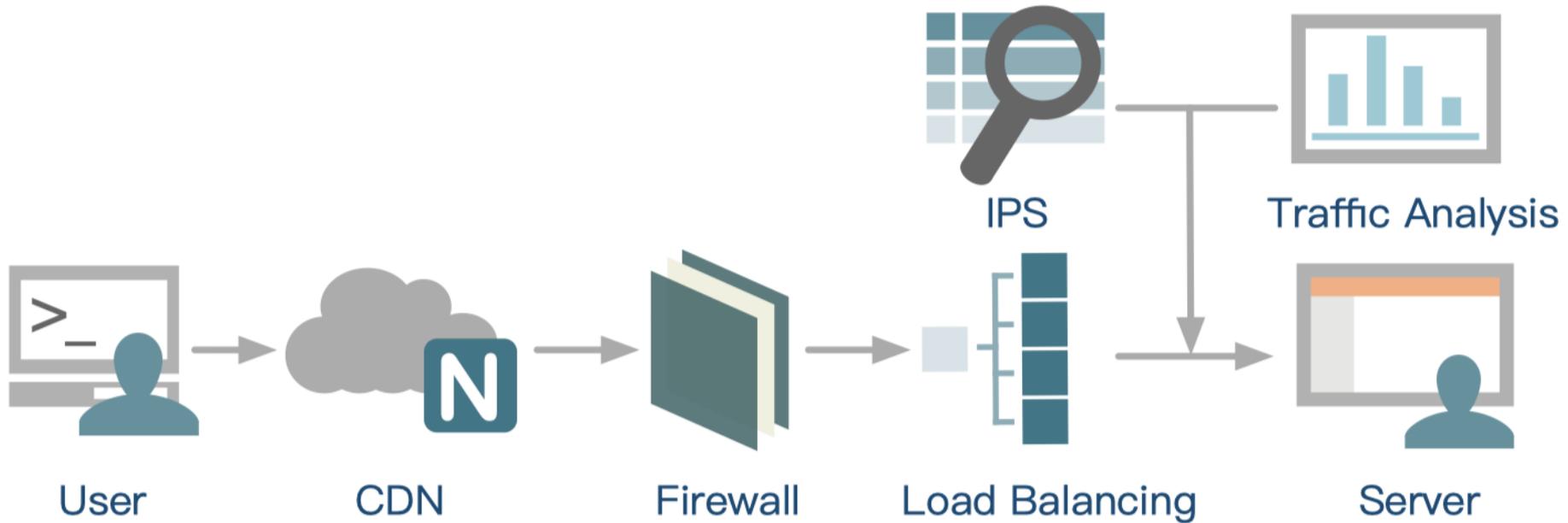
缓存污染/DOS攻击

注：细节非本次攻击原理

我们是如何发现此类攻击

How did we discover such attacks

复杂的Web网络环境



我们是如何发现此类攻击

How did we discover such attacks

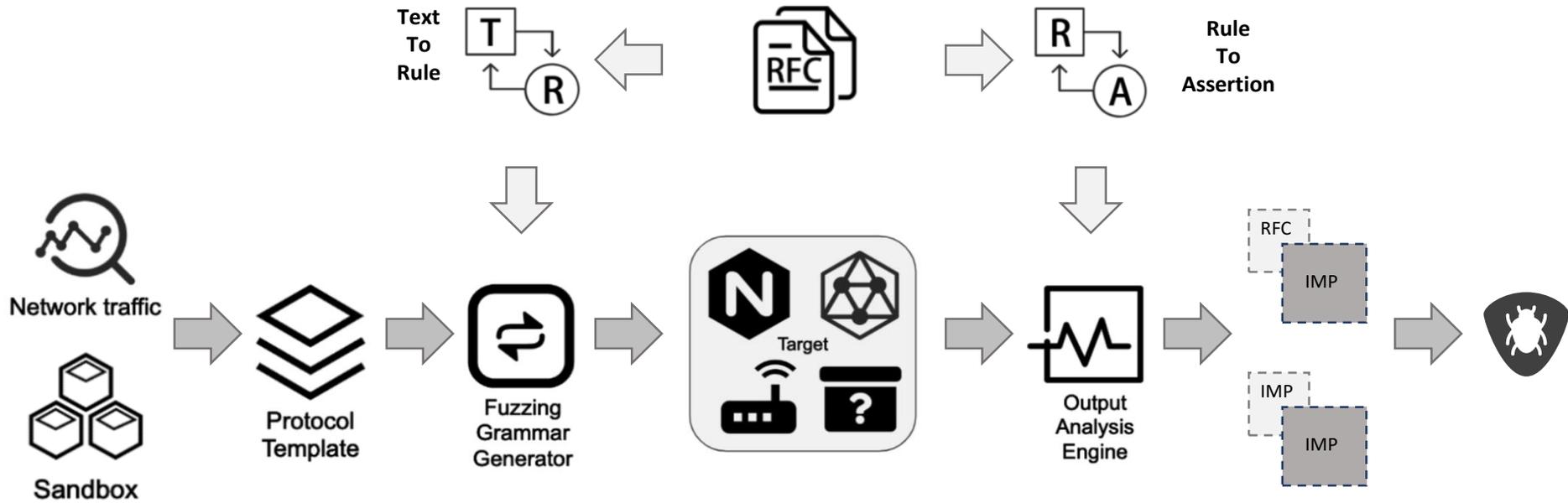
HTTP请求解析流程



我们是如何发现此类攻击

How did we discover such attacks

自动化测试框架





清华大学
Tsinghua University

感谢聆听！ 欢迎指正！

清华大学网络科学与网络空间研究院