[关闭]
@ensis 2016-01-21 17:38 字数 1422 阅读 111

Forwarding-Loop Attacks in Content Delivery Networks

NDSS'16

原文链接
作者信息：Jianjun Chen, Xiaofeng Zheng, Haixin Duan and Jinjin Liang (Tsinghua University) and Jian Jiang (University of California, Berkeley) and Kang Li (University of Georgia) and Tao Wan (Huawei Canada) and Vern Paxson (University of California, Berkeley and International Computer Science Institute)

Abstract

文章介绍了恶意用户通过创建CDN内或多个CDN间的forwarding-loop来攻击CDN的可用性。作者评估的16个CDN提供商全部受这种攻击的影响。尽管有些CDN有一些对应的检测措施，但都可以被绕过，并且攻击的防御需要所有CDN间的合作。此外，文章还讨论了单个CDN可以马上采取的措施。
在更高层次上，文章的工作强调了在用户有转发控制权，特别是没有单点管理控制的时候，networked system可能会有的问题。

- 贡献点：
  - 介绍forwarding-loop攻击
  - 对16个流行的CDn提供商进行测试
  - 提出Dam Flooding攻击，一种危害极高的forwarding-loop攻击
  - 提出应对或减轻攻击的方法

Background

CDN：提高网站性能和规模，提供安全特性如DDos保护、网络应用防火墙（WAF）。
涉及到CDN的网页访问可以分为两步，首先用户被引导到距离用户较近的CDN服务器上，之后CDN获取到内容返回给用户。
第一步叫做request routing，一般可以通过URL重写（网站所有者将网站URL改为CDN的子域名）或基于DNS的request routing（改变DNS对网站域名的解析，返回CDN服务器的IP或CNAME）实现。
第二步关心的是CDN如何获取到用户请求的内容，有两种模式push和pull，push指网站所有者自己把内容上传到CDN，而pull则是CDN服务器扮演反向代理的角色，在本地没有缓存的情况下，将请求转发到原始网站。

Forwarding-loop攻击

在pull模式中，恶意的CDN客户可以故意操纵forwarding过程，造成forwarding-loop。
在CDN节点转发客户的请求之前，会检查请求的Host头来获取客户指定的发送目的地，然后连

接发送目的地并转发请求。
如果攻击者故意将发送目的地设置成另一个CDN节点，那么发送过程就会继续，并且可能形成一个循环。
文章讨论了4种可以形成循环的方法：self loop；intraCDN loop；interCDN loop；CDN Dam Flooding。

	Self-Loop	Intra-CDN loop	Inter-CDN loop	Dam Flooding
Akamai			✓	✓
Alibaba			✓	✓
Azure (China)	✓	✓	✓	✓
Baidu			✓	✓
CDN77		✓	✓	✓
CDNlion		✓	✓	✓
CDN.net		✓	✓	✓
CDNsun		✓	✓	✓
CloudFlare			✓	✓
CloudFront			✓	✓
Fastly			✓	✓
Incapsula			✓	✓
KeyCDN	Likely	✓	✓	✓
Level3			✓	✓
MaxCDN	Likely	✓	✓	✓
Tencent			✓	✓

影响Forwarding-loop的因素

修改Host头

后续节点是否接受转发的请求依赖于Host头，按照是否修改host头forwarding-loop可以分为两类：一类是请求发出时是网站的原始域名，并且在转发到CDN节点时，CDN不对Host做修改

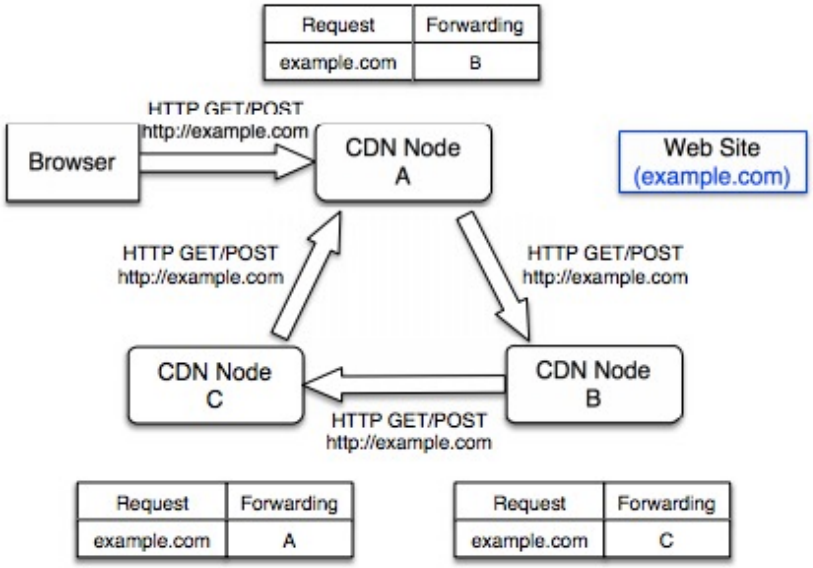

Fig. 2. A conceptual view of a CDN forwarding loop created by manipulating forwarding configuration: see Section III-B through Section III-E for the detailed mechanisms for constructing forwarding loops.

另一种是CDN会更改Host头来反映发送的目的地。当Host是IP时，没有CDN会接受这样的请求。

HOST MODIFICATION BEHAVIORS. *("N/A" indicates that the feature is either not available for testing due to our account's limitations, or not applicable.)*

	Request with CDN Subdomain		Request with Customer Domain	
	Forwarding to IP	Forwarding to Domain	Forwarding to IP	Forwarding to Domain
Akamai	N/A		Configurable	
Alibaba	Configurable		Configurable	
Azure (China)	N/A		Request Domain	
Baidu	N/A		Request Domain	
CDN77	Request Domain	Forwarding Domain	Request Domain	Forwarding Domain
CDNlion	Request Domain	Forwarding Domain	Request Domain	Forwarding Domain
CDN.net	Request Domain	Forwarding Domain	Request Domain	Forwarding Domain
CDNsun	Request Domain	Forwarding Domain	Request Domain	Forwarding Domain
CloudFlare	N/A		Request Domain	
CloudFront	N/A	Request Domain	N/A	Forwarding Domain
Fastly	N/A		Request Domain	
Incapsula	N/A		Request Domain	N/A
KeyCDN	**Forwarding IP**	Forwarding Domain	Request Domain	Forwarding Domain
Level3	N/A		N/A	Request Domain
MaxCDN	**Forwarding IP**	Forwarding Domain	Configurable	
Tencent	N/A		Request Domain	

修改其他头字段

TABLE III. HEADER (EXCEPT HOST) MODIFICATION BEHAVIORS

	Size Increase	Loop Detection	Reset	Filtering
Akamai	Via, X-Forwarded-For	Akamai-Origin-Hop		
Alibaba	Via, X-Forwarded-For	Via		
Azure (China)	X-Forwarded-For			
Baidu	X-Forwarded-For	X-Forwarded-For, CF-Connecting-IP		
CDN77	X-Forwarded-For		Via	
CDNlion	X-Forwarded-For		Via	
CDN.net	X-Forwarded-For		Via	
CDNsun	X-Forwarded-For		Via	
CloudFlare	X-Forwarded-For	X-Forwarded-For, CF-Connecting-IP		
CloudFront	Via, X-Forwarded-For	Via		
Fastly	Fastly-FF, X-Varnish	Fastly-FF		Non-self-defined
Incapsula	Incap-Proxy-ID, X-Forwarded-For	Incap-Proxy-ID		
KeyCDN			X-Forwarded-For	
Level3	Via, X-Forwarded-For	Via		
MaxCDN				Any header
Tencent		X-Daa-Tunnel		

CDN对收到的请求长度有限制。

TABLE IV. HEADER SIZE LIMITATION (SINGLE/ALL HEADERS)

Vendor	Limitation	Vendor	Limitation
Akamai	16KB/16KB	CloudFlare	32KB/92KB
Alibaba	32KB/64KB	CloudFront	24KB/24KB
Azure (China)	20KB/20KB	Fastly	64KB/64KB
Baidu	32KB/92KB	Incapsula	25KB/>1600KB
CDN77	16KB/64KB	KeyCDN	8KB/32KB
CDNlion	16KB/64KB	Level3	9KB/12KB
CDN.net	16KB/64KB	MaxCDN	32KB/156KB
CDNsun	16KB/64KB	Tencent	6KB/6KB

处理timeout

TABLE V. FORWARDING TIMEOUTS AND THE ADOPTION OF ABORT FORWARDING.

	Forwarding Timeout (second)	Abort Forwarding
Akamai	240	
Alibaba	60	✓
Azure (China)	900	✓
Baidu	100	✓
CDN77	60	
CDNlion	60	
CDN.net	60	
CDNsun	60	
CloudFlare	100	✓
CloudFront	90	✓
Fastly	configurable (max 75)	
Incapsula	360	✓
KeyCDN	60	✓
Level3	60	
MaxCDN	60	✓
Tencent	10	✓

DNS解析

Non-streaming与streaming

TABLE VII. SUPPORT OF HTTP STREAMING.

	Request Streaming	Response Streaming
Akamai	✓	✓
Alibaba	✓	✓
Azure (China)	✓	✓
Baidu		✓
CDN77		✓
CDNlion		✓
CDN.net		✓
CDNsun		✓
CloudFlare		✓
CloudFront	✓	✓
Fastly	✓	✓
Incapsula	✓	✓
KeyCDN		✓
Level3	✓	✓
MaxCDN		✓
Tencent		✓

- 内容目录

-

-
  - AsiaCCS15 1
  - Lucky 13 Strikes Back
  - CCS'14 1
  - ShadowCrypt: Encrypted Web Applications for Everyone
  - IMC2015 1
  - Neither Snow Nor Rain Nor MITM . . . An Empirical Analysis of Email Delivery Security
  - MoST'15 1
  - AppCracker: Widespread Vulnerabilities in User and Session Authentication in Mobile Apps
  - NDSS'16 2
  - Forwarding-Loop Attacks in Content Delivery Networks
  - TLS in the wild: An Internet-wide analysis of TLS-based protocols for electronic communication
  - SOUPS15 1

- “I Added ‘!’ at the End to Make It Secure”:Observing Password Creation in the Lab
- SSL 2
  - TLS扩展的那些事
  - SSL的Padding Oracle攻击
- SSLVPN 1
  - SSL中间人框架——风声的基本介绍
- SSL文章2016 1
  - 四大SSL相关文章整理（六）
- Security'14 1
  - SpanDex: Secure Password Tracking for Android
- Security'15 1
  - Cookies Lack Integrity: Real-World Implications
- cve 2
  - CVE-2016-0800: DROWN ATTACK
  - 关于OpenSSL CVE-2016-0701漏洞的分析
- gossip漏洞报告 1
- [illegible]nDown漏洞报告
- 以下【标签】将用于标记这篇文稿：
  - “I Added ‘!’ at the End to Make It Secure”:Observing Password Creation in the Lab
- 推送 1
  - 个推协议分析
- 下载客户端
- 关注开发者
- 报告问题，建议
- 联系我们

搜索 ensis 的文稿标题，* 显

password

添加新批注

保存 取消

在作者公开此批注前，只有你和作者可见。

保存 取消

修改 保存 取消 删除

- 私有
- 公开
- 删除

查看更早的 5 条回复

回复批注