域名前置(Domain Fronting)

1 概念介绍

Domain Fronting 是一种为逃避审查机制而出现的网络技术，其基本原理是利用合法且高度可信的第三方服务来转发客户端和目标服务器之间的网络流量，从而躲避流量审查；其核心思想是在不同的通信层使用不同的域名。

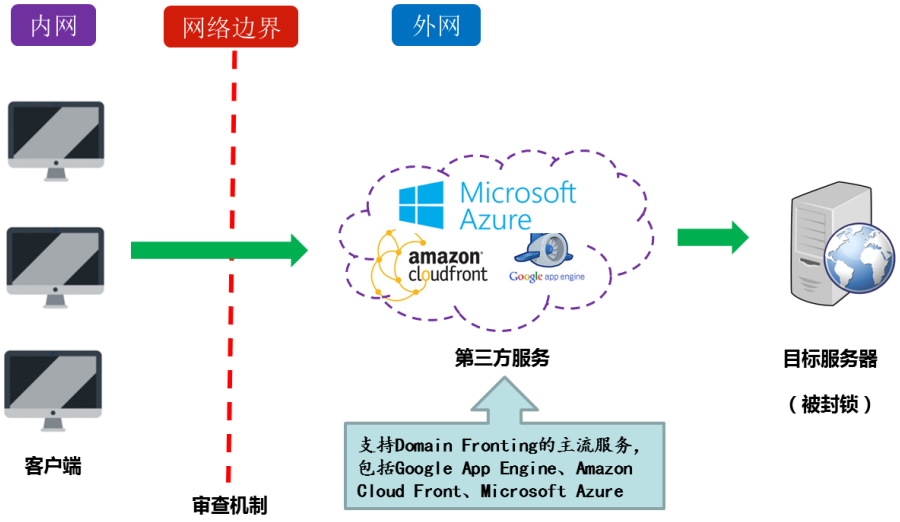

图 1 Domain Fronting 运行流程

通常，在我们通过域名访问 HTTPS 网站的过程中，目标服务器的域名会在三个位置出现：DNS 查询请求、TLS SNI（Server Name Indication）、HTTP 请求头的 Host 字段。

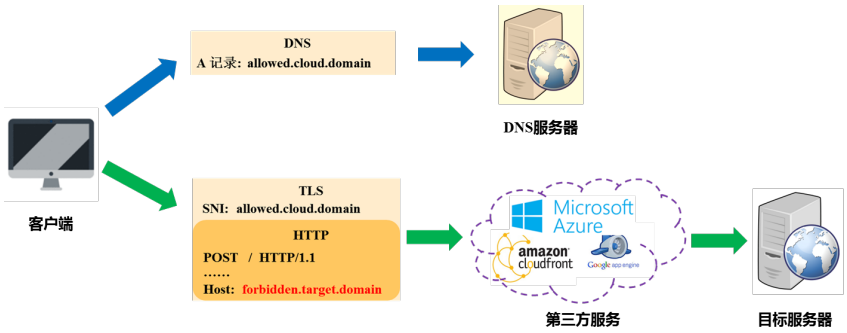

图 2 Domain Fronting 基本原理

基于 Domain Fronting 技术，真正要访问的目标服务器的域名隐藏在 HTTP

请求头的 HOST 字段且该被 TLS 层加密，其对审查设备而言是不可见的。当第三方服务接收到客户端请求后，会解密该请求的 TLS 层，之后根据内部 HTTP 头中的 Host 字段将请求转发给指定的目标服务器。相对于普通的代理服务器，该机制的优势在于：审查机构要想彻底屏蔽被封锁的目标服务器，则需屏蔽提供该服务的一大堆主流网络服务商，其附带损害相对较大。

2 实际案例

目前，已经出现利用 Domain Fronting 技术用于网络攻击的活动。据 FireEye 于 2017 年 3 月 27 日发布的报告，俄罗斯网络间谍组织 APT29 至少在两年之前就已经开始使用 Domain Fronting 技术，以加大目标组织对恶意流量的识别难度。

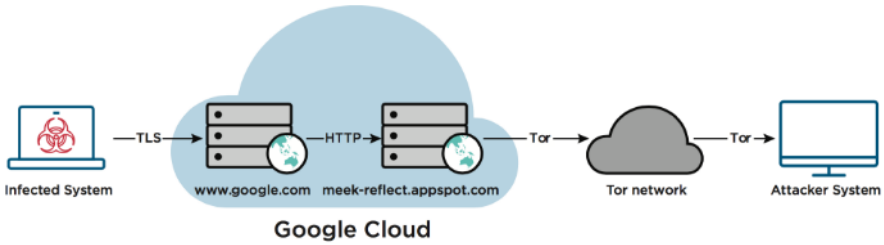

图 3 使用 meek 的流量路线

APT29 利用 Tor 网络与受感染设备进行通信，为了将 Tor 流量伪造为合法流量，该组织使用了 Meek——一款实现了 Domain Fronting 技术的 Tor 流量混淆插件。该插件可以将 Tor 流量进一步伪装成基于 HTTPS 加密的云服务流量，从而隐藏 Tor 流量的指纹特征，其允许被感染客户端在一条指向 www.google.com（或 a0.awsstatic.com、ajax.aspnetcdn.com 等）的看似无害 HTTPS POST 请求内发送实际指向 Tor 的流量。

3 原理分析

本文用DFM代表支持Domain Fronting的Malware ;用M代表普通的Malware；用 cc.com 代表由 BotMaster 控制的 C&C 服务器域名；用 S 代表部署在网络边界的内容审查系统、异常检测系统等安全基础设施(Security Infrastructure)；用 W 代表未被 S 屏蔽且支持 Domain Fronting 的第三方服务器。

（1）M 的运行流程

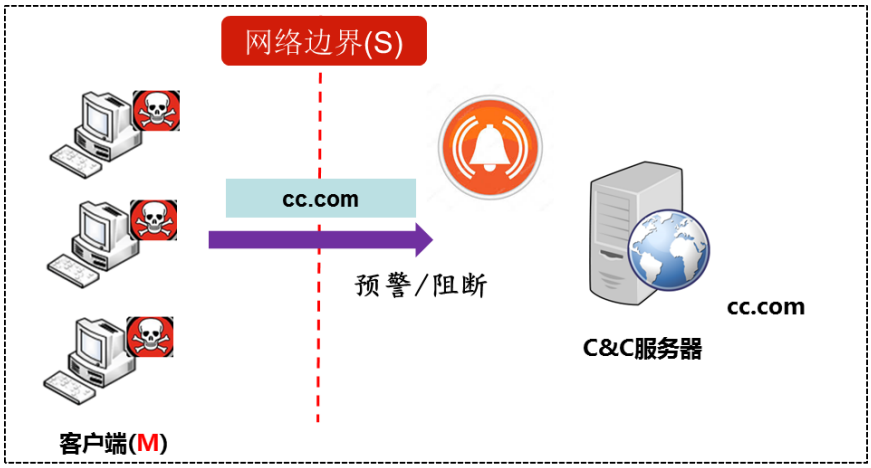

图 4　M 运行流程（1）

对于 M 而言，当其开始运行时，会通过 cc.com 直接联系 C&C 服务器。一般情况下，cc.com 是一个十分生僻的域名（多数知名 APT 事实上都在访问生僻域名），此时，部署在网络边界的 S 可能会发现该异常流量进而进行预警或阻断。而一旦该域名被阻断，M 便会因与 C&C 服务器失去联系而失效。

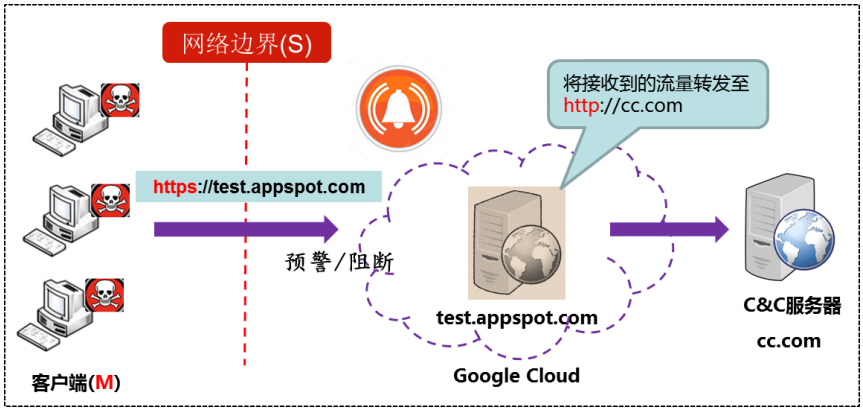

图 5　M 运行流程（2）

此时为绕过 S 的限制，BotMaster 可通过第三方提供的服务（如:Google App Engine、Amazon Cloud Front、CloudFlare 等）来转发客户端 M 和 C&C 服务器之间的流量。以 Google App Engine 为例，需要 BotMaster 进行的相关操作包括：配置一个项目并部署（具有流量转发功能的）Web 应用程序到该项目。其中，(1) 配置项目时，Google App Engine 会为该项目生成以 appspot.com 结尾的子域名，如 :test.appspot.com，该子域名即为所部署 Web 应用程序的网址；(2) 所部署 Web 应用程序的功能仅仅是转发流量，其在代码层面会配置 cc.com 的主机地址，凡是发往 test.appspot.com 的流量都会被转发到 cc.com 对应的主机，即访问 test.appspot.com 的效果等同于访问 cc.com。因此，对于客户端 M 来说，如果 cc.com 被 S 屏蔽，其便可通过 test.appspot.com 间接与 C&C 服务器取得联系。

虽然客户端 M 可通过 test.appspot.com 联系 C&C 服务器，但这并未体现 Domain Fronting 技术。因为当 S 发现 test.appspot.com 存在恶意行为时，依然可将其添加到黑名单之中。此时，为再次绕过 S 的限制，需要 BotMaster 在 GAE 上配置新的项目，使用新生成的子域名，该过程比较繁琐，而且消耗资源。此外，当 S 选择将 appspot.com 添加到黑名单，而不仅是该域名的某一特定子域名时，那么即使使用新生成的子域名，也无法绕过 S 的限制。而对于 DFM 来说，其可通过支持 Domain Fronting 的服务器 W，打破这种限制。

（2）DFM 运行流程

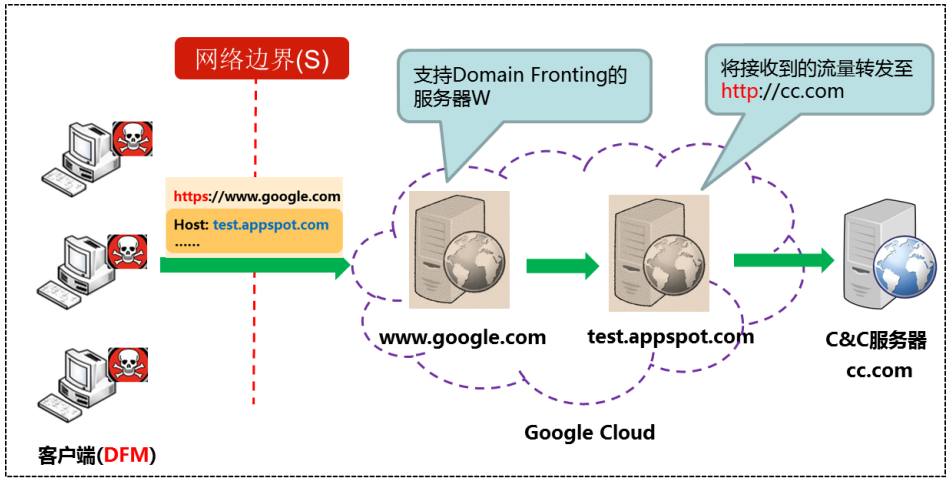

图 6　DFM 的运行流程

对于 DFM 而言，当其开始运行时，其即不会通过 cc.com，也不过通过 test.appspot.com 联系 C&C 服务器，而是通过支持 Domain Fronting 的服务器 W 与 C&C 服务器联系。以 Google 为例，其支持 Domain Fronting 的该类服务器有:www.google.com、gmail.google.com、maps.google.com、youtube.com、ssl.google-analytics.com 等。当 DFM 开始运行, DFM 会将 test.appspot.com (而不是 cc.com, 其原因是服务器 W 不会随意转发流量，只会向匹配一定规则的域名转发流量，即:其允许向*.appspot.com 转发流量，但不会向 cc.com 转发流量，因此需要二次转发)封装起来, 然后联系支持 Domain Fronting 的服务器 W (www.google.com), 由 W 将收到的流量解密，再转发给 test.appspot.com，最终该请求会被转发到 ccc123.com 对应的主机。在细节层面，test.appspot.com 被封装在发往 W(www.google.com)的 HTTP 请求的 Host 字段且经过 TLS 层加密，其对审查设备 S 而言是不可见的。

防御人员要想屏蔽 DFM 与 C&C 服务器之间的联系，则需要屏蔽所有支持 Domain Fronting 的服务器 W，仅屏蔽*.appspot.com 或 cc.com 是没有效果的。因

为 DFW 并不与*.appspot.com 或 cc.com 直接联系。如上所述，Google 的该类服务器有：www.google.com、gmail.google.com、maps.google.com、youtube.com、ssl.google-analytics.com 等，如果屏蔽这些主流站点，相当于屏蔽了 S 内部用户对互联网的访问，其附带损害较大，因此防御方通常并不会封锁这些站点。而正是由于防御方所存在的附带损害，对于攻击者而言，当网络中部署多种防御方案时，比如：防火墙、IPS、IDS 等，基于 Domain Fronting 技术可有效绕过这些方案的限制。

4 小结

对于攻击者而言，当网络中部署多种防御方案的时候，比如：防火墙、IPS、IDS 等，使用 Domain Fronting 技术可有效绕过这些方案的限制；对于防御者而言，当攻击者使用该技术以规避安全检测的时候，很难在通信流量中判断一个域名是否使用了 Domain Fronting 技术，目前尚未出现有效的防御方案；对于支持该技术的云平台服务商而言，为避免其被恶意的攻击者所使用，应加大审核力度，提高注册该服务的门槛。