一、基本问题

1、被感染的Windows虚拟机的IP

答案

172.16.165.132

分析思路

通过过滤"http.request",找到所有发起http请求的主机,发现只有172这台主机

2014-11-23-traffic-analysis-exercise.pcap 文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H) http.request Protocol Length Status Code Info No. Time Source Destination 1 0.00000 172.16.165.132 74.125.230.120 HTTP 743 GET /url?sa=t&rct=j&q=&esrc=s&frm=1&sour GET /favicon.ico HTTP/1.1

525 GET / HTTP/1.1

365 GET /wp-content/themes/comicpress-hijink

384 GET /wp-content/plugins/eshop-order-emai

397 GET /wp-content/themes/comicpress-hijink

380 GET /wp-content/plugins/wp-lightbox-2/st

366 GET /wp-content/plugins/jetpack/css/jetp

355 GET /button/buttons.js HTTP/1.1

373 GET /wp-content/plugins/comic-easel/css/

386 GET /wp-content/plugins/comic-easel/imag

354 GET /wp-content/uploads/eshop_files/esho 4 0.332042 172.16.165.132 18 1.187319 172.16.165.132 23 1.578633 172.16.165.132 GET /favicon.ico HTTP/1.1 74.125.230.120 HTTP 514 18 1.187319 192.30.138.146 HTTP 23 1.578633 192.30.138.146 HTTP 172.16.165.132 172.16.165.132 172.16.165.132 172.16.165.132 172.16.165.132 48 1.962023 192.30.138.146 HTTP 50 1.962196 192.30.138.146 HTTP 52 1.962330 192.30.138.146 HTTP 54 1.962505 192.30.138.146 HTTP 69 2.202491 88,221,134,170 HTTP 172.16.165.132 172.16.165.132 172.16.165.132 172.16.165.132 74 2.225348 192.30.138.146 HTTP 78 2.226140 192.30.138.146 HTTP 354 382 80 2.226657 192.30.138.146 HTTP GET /wp-content/uploads/eshop files/esho 83 2.325533 192.30.138.146 HTTP GET /wp-content/plugins/mf-gig-calendar/ 125 2.570113 172.16.165.132 192.30.138.146 381 GET /wp-includes/js/jquery/jquery.js?ver HTTP

2、受感染虚拟机的MAC地址

答案

00:50:56:f3:ca:52

分析思路

查看关于IP172.16.165.132数据包中数据链路层的MMAC地址

	78 2.226140	172.16.165.132	192.30.138.146	HTTP	386	GET /wp-content/
	80 2.226657	172.16.165.132	192.30.138.146	HTTP	354	GET /wp-content/
	83 2.325533	172.16.165.132	192.30.138.146	HTTP	382	GET /wp-content/
	125 2.570113	172.16.165.132	192.30.138.146	HTTP	381	GET /wp-includes
	133 2.572244	172.16.165.132	192.30.138.146	HTTP	392	GET /wp-includes
	134 2.572356	172.16.165.132	192.30.138.146	HTTP	412	GET /wp-content/
	163 2.693527	172.16.165.132	192.30.138.146	HTTP	409	GET /assets/misc
	165 2.693706	172.16.165.132	192.30.138.146	HTTP	353	GET /jumpbar.js
	167 2.693861	172.16.165.132	192.30.138.146	HTTP	440	GET /wp-content/
	172 2.716778	172.16.165.132	192.30.138.146	HTTP	434	GET /wp-content/
<	*05.0.0000*	470 46 465 430			***	CET / 1 / 1
		. (0000 1:1	\	(2222 11	`	

- > Frame 54: 366 bytes on wire (2928 bits), 360 bytes captured (2928 bits)
- > Ethernet II, Src: VMware_c5:b7:a1 (00:0c:29:c5:b7:a1) Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
- > Internet Protocol Version 4, Src: 172.16.165.132, Dst: 192.30.138.146
- > Transmission Control Protocol, Src Port: 49371, Dst Port: 80, Seq: 1, Ack: 1, Len: 312
- > Hypertext Transfer Protocol

3、受感染网站的IP地址

答案

192.30.138.146

分析过程

前面的分析均为跳包模式,现在从头开始追包,可以看到序号1-5包一直与IP 74.125.230.120进行交互,在序号6包、序号11包时出现了一条192.30.138.146的DNS解析记录,之后频繁与该IP进行交互,初步确认为受感染的IP

٥.	Time	Source	Destination	Protocol	Length Status Code	e Info			
	1 0.000000	172.16.165.132	74.125.230.120	HTTP	743	GET /url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=			
	2 0.000192	74.125.230.120	172.16.165.132	TCP	60	80 → 49361 [ACK] Seq=1 Ack=690 Win=64240 Len=0			
	3 0.306675	74.125.230.120	172.16.165.132	HTTP	880 2	00 HTTP/1.1 200 OK (text/html)			
	4 0.332042	172.16.165.132	74.125.230.120	HTTP	514	GET /favicon.ico HTTP/1.1			
	5 0.332197	74.125.230.120	172.16.165.132	TCP	60				
	6 0.351533	172.16.165.132	172.16.165.2	DNS	76	Standard query 0xf082 A hijinksensue.com			
	7 0.644953	74.125.230.120	172.16.165.132	TCP	1409	80 → 49361 [PSH, ACK] Seq=827 Ack=1150 Win=64240 Len=1355 [TCP segment			
	8 0.745024	74.125.230.120	172.16.165.132	TCP	1409	[TCP Retransmission] 80 → 49361 [PSH, ACK] Seq=827 Ack=1150 Win=64240			
	9 0.745049	172.16.165.132	74.125.230.120	TCP	54	49361 → 80 [ACK] Seq=1150 Ack=2182 Win=64240 Len=0			
	10 0.766567	74.125.230.120	172.16.165.132	HTTP	87 2	00 HTTP/1.1 200 OK (image/x-icon)			
	11 0.766620	172.16.165.2	172.16.165.132	DNS	92	Standard query response 0xf082 A hijinksensue.com A 192.30.138.146			
	12 0.767192	172.16.165.132	192.30.138.146	TCP	66	49366 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1			
	13 0.767331	172.16.165.132	192.30.138.146	TCP	66	49367 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1			
	14 0.866550	74.125.230.120	172.16.165.132	TCP	87	[TCP Retransmission] 80 → 49361 [PSH, ACK] Seq=2182 Ack=1150 Win=64240			
	15 0.866570	172.16.165.132	74.125.230.120	TCP	54	49361 → 80 [ACK] Seq=1150 Ack=2215 Win=64207 Len=0			
	16 1.185297	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460			
	17 1.185343	172.16.165.132	192.30.138.146	TCP	54	49367 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0			
	18 1.187319	172.16.165.132	192.30.138.146	HTTP	525	GET / HTTP/1.1			
	19 1.187484	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [ACK] Seq=1 Ack=472 Win=64240 Len=0			
	20 1.305954	192.30.138.146	172.16.165.132	TCP	60	80 → 49366 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460			
		170 15 155 170	*** *** ***			tones on figure of the second of			
	0101 = Hea	der Length: 20 bytes	(5)						
>	Differentiated:	Services Field: 0x00	(DSCP: CS0, ECN: Not	-ECT)					
	Total Length: 4	9							
	Identification:	0x15d7 (5591)							
>	Flags: 0x40, Do	n't fragment							
	0 0000 0000								
	Time to Live: 1	ime to Live: 128							
	Protocol: TCP (6)								
	Header Checksum: 0x48b3 [validation disabled]								
	[Header checksu	Header checksum status: Unverified]							
	Source Address:		'						
Destination Address: 192.30.138.146									

4、被入侵网站的域名

答案

hijinksensue.com

分析过程

查看关于上面IP的DNS记录或HTTP数据包中的Host值,可以看到域名为hijinksensue.com

						(12 10 1 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
1 0.000000		74.125.230.120	HTTP	743		/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=ht				
2 0.000192		172.16.165.132	TCP	60		49361 [ACK] Seq=1 Ack=690 Win=64240 Len=0				
3 0.306675		172.16.165.132	HTTP	880		/1.1 200 OK (text/html)				
4 0.332042		74.125.230.120	HTTP	514		/favicon.ico HTTP/1.1				
5 0.332197		172.16.165.132	TCP	60		49361 [ACK] Seq=827 Ack=1150 Win=64240 10=0				
6 0.351533		172.16.165.2	DNS	76		dard query 0xf082 A hijinksensue.com				
7 0.644953		172.16.165.132	TCP	1409		49361 [PSH, ACK] Seq=827 Ack=1150 Win=64240 Len=1355 [TCP segment o				
8 0.745024		172.16.165.132	TCP	1409		Retransmission] 80 → 49361 [PSH, ACK] Seq=827 Ack=1150 Win=64240 Le				
9 0.745049		74.125.230.120	TCP	54		1 → 80 [ACK] Seq=1150 Ack=2182 Win=64240 Len=0				
10 0.766567		172.16.165.132	HTTP	87		/1.1 200 OK (image/x-icon)				
11 0.766620		172.16.165.132	DNS	92		dard query response 0xf082 A hijinksensue.com A 192.30.138.146				
12 0.767192		192.30.138.146	TCP	66		66 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1				
13 0.767331	172.16.165.132	192.30.138.146	TCP	66	4936	77 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1				
15 0.70				TCP	00	אר סרד-כרון מאר דפרון מרוו-סדאר דפרון מין באר (מונים) אר אריבים ארוו-סדאר דפרון מין באר				
14 0.86				TCP	87	[TCP Retransmission] 80 → 49361 [PSH, ACK] Seq=2182 Ack=1				
15 0.86	6570 172.16.165.13	32 74.125.236	.120	TCP	54	49361 → 80 [ACK] Seq=1150 Ack=2215 Win=64207 Len=0				
16 1.18	5297 192.30.138.14	46 172.16.165	.132	TCP	60	80 → 49367 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146				
17 1.18	5343 172.16.165.13	32 192.30.138	.146	TCP	54	49367 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0				
→ 18 1.18	7319 172.16.165.13	32 192.30.138	3.146	HTTP	525	GET / HTTP/1.1				
19 1.18	7484 192.30.138.14	46 172.16.165	.132	TCP	60	80 → 49367 [ACK] Seq=1 Ack=472 Win=64240 Len=0				
20 4 30	FOF4 400 30 430 4	×c /22 ×c ×c	433	TOD		00 40000 [000] 400] 0 0 4-0 4 10- 04040 1 0 400 440				
(/								
> GET / HT	TP/1.1\r\n									
Accept:	text/html, application/	/xhtml+xml, */*\r\n								
Referer:	http://www.google.co.u	//url?sa=t&rct=i&d	=&esrc=s8	kfrm=1&sou	rce=web&cd=1	&ved=0CCEQFjAA&url=http%3A%2F%2Fhijinksensue.com%2F&ei=LjFxVOC5				
	anguage: en-US\r\n	,								
	Accept-ganguage. ein-ss (ii) User-Agent: Mozilla/5.0 (cg/batible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)\r\n									
Accept-Encoding: gzip, deflate\r\n										
Host: hijinksensue.com\r\n										
Connection: Keep-Alive\r\n										
\r\n										
<pre>[Full request URI: http://hijinksensue.com/]</pre>										
[HTTP re	[HTTP request 1/7]									
[Response in frame: 123]										
	[Next request in frame: 125]									

5、提供恶意软件的IP地址和域名

答案

37.143.15.180

g.trinketking.com:51439

分析过程1

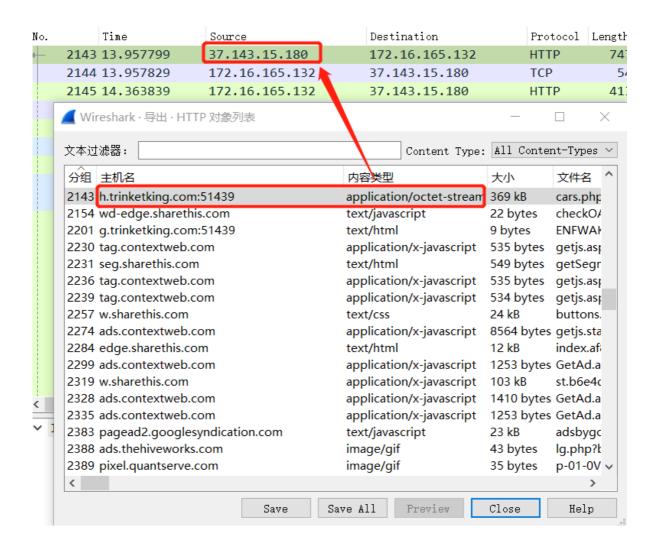
导出值 -> http,可以看到一个文件类型为"application/octet-stream"的文件,导出时直接被安全软件查杀了,其他文件均为正常的图片/文档。可以看到该恶意软件提供的主机名为"h.trinketking.com:51439"



■ Wireshark · 导出 · HTTP 对象列表 Content Type: All Content-Types ~ 文本过滤器: 分组 主机名 内容类型 大小 文件名 1652 pixel.wp.com image/gif 50 bytes url%3Fsa 1675 hijinksensue.com 2790 bytes prev.png image/png 1680 hijinksensue.com image/jpeg 33 kB saf-quid 1691 hijinksensue.com 10 kB amazon image/png 1692 g.trinketking.com:51439 137 kB text/html birds.ph 1703 hijinksensue.com image/png 3034 bytes lastin.pn 1705 ads.thehiveworks.com application/javascript 6707 bytes fl.js 1706 wd-edge.sharethis.com text/javascript 162 bytes getAllAr image/png 1710 hijinksensue.com 2731 bytes next.pnc application/octet-stream 369 kB 2143 h.trinketking.com:51439 cars.php 2154 wd-edge.sharethis.com checkO/ text/javascript 22 bytes 2201 g.trinketking.com:51439 text/html 9 bytes **ENFWAH** 2230 tag.contextweb.com application/x-javascript 535 bytes getjs.ası 2231 seg.sharethis.com text/html 549 bytes getSegr 2236 tag.contextweb.com application/x-javascript 535 bytes getjs.ası 2239 tag.contextweb.com application/x-javascript 534 bytes getjs.ası 2257 w.sharethis.com text/css 24 kB buttons. v Save All Save Preview Close Help

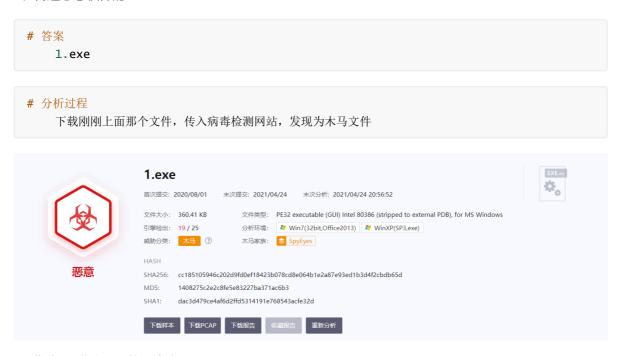
分析过程2

定位该数据包,可以看到该恶意软件提供的IP



二、高级问题

1、传递恶意软件的EK

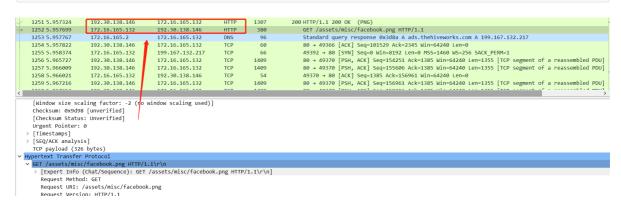


2、指向EK登陆页面的重定向URL

答案 hijinksensue.com/assets/misc/facebook.png

分析过程

通过查看恶意软件IP出现的第一个HTTP数据包(没有发现Referer头),在其之上虚拟机做了一次DNS解析与该IP进行连接,在该DNS解析前向192.30.138.146发出了请求,初步判断是从该位置跳转过来的



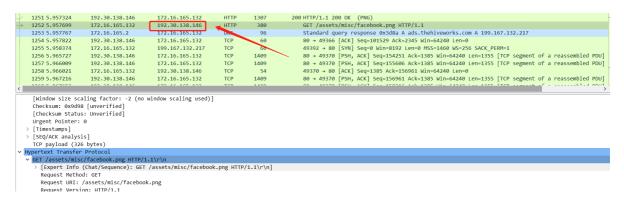
3、指向EK登录页面的重定向URL的IP

答案

192.30.138.146

分析过程

取上一个答案的IP



4、pcap提交Virus Total并触发的snort警报

Snort Alerts

Senstive Data

(spp_sdf) SDF Combination Alert [1]

Potentially Bad Traffic

(http_inspect) LONG HEADER [19]

PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority [254]

Attempted Administrator Privilege Gain

SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt [2381]
SERVER-APACHE Apache Struts wildcard matching OGNL remote code execution attempt [29639]

Attempted User Privilege Gain

BROWSER-PLUGINS AcroPDF.PDF ActiveX clsid access attempt [13913]

BROWSER-IE Microsoft Internet Explorer XHTML element memory corruption attempt [13974]

BROWSER-IE Microsoft Internet Explorer HTML DOM invalid DHTML textnode creation attempt [16301]

PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt [19187]

INDICATOR-OBFUSCATION Multiple character encodings detected [29509]

POLICY-OTHER PDF ActiveX CLSID access detected [38038]

FILE-IMAGE Apple PICT Quickdraw image converter packType 4 buffer overflow attempt [44455]

SERVER-OTHER Beetel Connection Manager username buffer overflow attempt [44679]

- + Potential Corporate Privacy Violation
- + A Network Trojan was detected
- + Detection of a Denial of Service Attack

5、提取恶意软件的Payload, MD5或SHA256哈希是什么

答案

MD5:1408275c2e2c8fe5e83227ba371ac6b3

SHA256:cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d

分析过程

提交该恶意软件到病毒分析平台,可直接查看到分析出的MD5值和SHA256值等

