如何去防御冰蝎 Webshell 管理工具

Vr-system

1、介绍

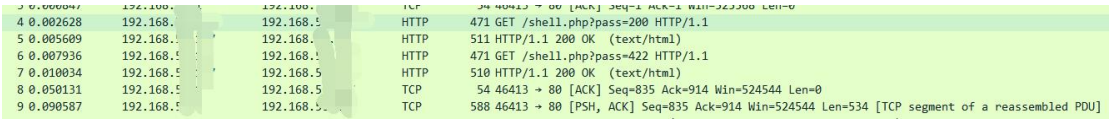
冰蝎 Webshell 管理工具是一款基于加密技术黑客工具，经常被人用作网站的后门管理工具，他的加密传输特性被用来绕过 IDS 或 IPS 等等的安全防护程序。的确加密技术对于安全防护程序的解密产生瓶颈。

2、关于冰蝎的分析

关于如何防御的方法，我是在 2018 的 12 月底开始的研究，2019 年的年初提出防御方法，并且将防御方法已经融合到我们的天融信产品之中。通过研究冰蝎的交互流程如下:

3、关于冰蝎的防御

防御方法之一在申请密钥请求和密钥反馈客户端联合判断，抓包分析如下：



4	0.002628	192.168.	192.168.5	HTTP	471 GET /shell.php?pass=200 HTTP/1.1
5	0.005609	192.168.	192.168.	HTTP	511 HTTP/1.1 200 OK (text/html)
6	0.007936	192.168.5	192.168.1	HTTP	471 GET /shell.php?pass=422 HTTP/1.1
7	0.010034	192.168.5	192.168.5	HTTP	510 HTTP/1.1 200 OK (text/html)
8	0.050131	192.168.5	192.168.5	TCP	54 46413 → 80 [ACK] Seq=835 Ack=914 Win=524544 Len=0
9	0.090587	192.168.5	192.168.5	TCP	588 46413 → 80 [PSH, ACK] Seq=835 Ack=914 Win=524544 Len=534 [TCP segment of a reassembled PDU]

冰蝎或进行两次交互，返回两次数据，数据内容由明显特征。

```
GET /shell.php?pass=200 HTTP/1.1
Content-type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; In
.NET4.0C; Tablet PC 2.0; .NET4.0E)
Host: 192.168.
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 09 Jul 2019 09:36:36 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
X-Powered-By: PHP/5.2.17
Set-Cookie: PHPSESSID=b4e1e8821994f70d834                    ; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 16
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

a7f1f14b5ccdce0aGET /shell.php?pass=422 HTTP/1.1
```