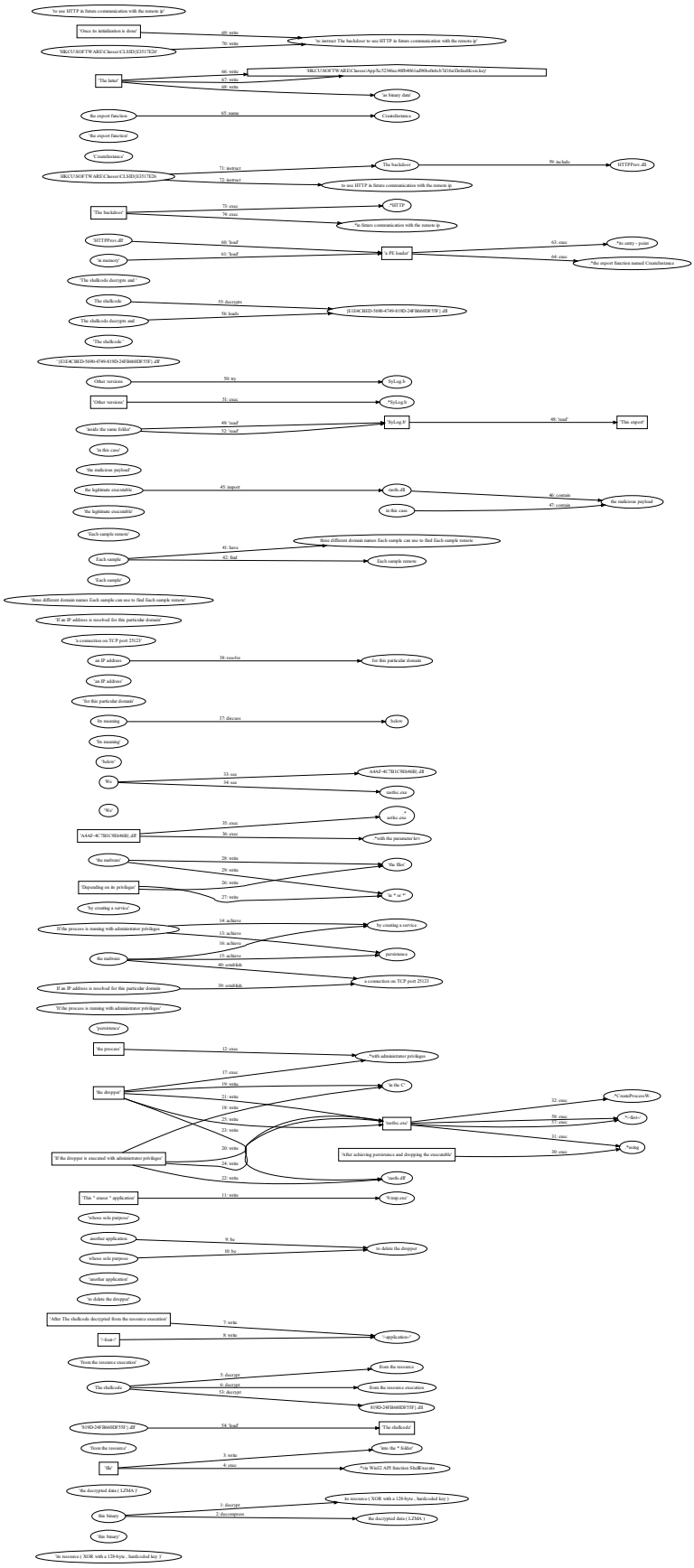
'to use HTTP in future communication with the remote ip'
Once its installation is done'
69: write
70: write
'to instruct The backdoor to use HTTP in future communication with the remote ip'
'HKCU\SOFTWARE\Classes\CLSID\{5351782b'
'HKCU\SOFTWARE\Classes\AppAx\5234ace40f0406ca8b0cabe4c5d16eDefaultIcon.key'
66: write
67: write
68: write
'The latter'
'in binary data'
'the export function'
65: name
'CreateInstance'
'the export function'
'CreateInstance'
'The backdoor'
59: include
HTTPPort.dll
71: instruct
72: instruct
'HKCU\SOFTWARE\Classes\CLSID\{5351782b'
'to use HTTP in future communication with the remote ip'
75: exec
76: exec
'The backdoor'
'%HTTP'
'to future communication with the remote ip'
HTTPPort.dll
60: load
61: load
'in memory'
'a PE loader'
63: exec
'*to entry - point'
64: exec
'*the export function named CreateInstance'
'The shellcode decrypts and'
The shellcode
55: decrypts
56: loads
'The shellcode decrypts and'
{E1E4C3ED-5690-4749-81ED-24F8b60DF55F}.dll
The shellcode
'{E1E4C3ED-5690-4749-81ED-24F8b60DF55F}.dll'
Other versions
50: try
%Log.log%
Other versions
51: exec
'%Log.log%'
'works the same folder'
49: load
52: load
%Log.log%
48: load
'This exploit'
'In this case'
'the malicious payload'
the legitimate executable
45: import
msfc.dll
46: contain
47: contain
the malicious payload
the legitimate executable
In this case
'Each sample retrieve'
'these different domain names Each sample can use to find Each sample retrieve'
Each sample
41: have
42: find
Each sample retrieve
Each sample
'these different domain names Each sample can use to find Each sample retrieve'
'If an IP address is resolved for this particular domain'
'a connection on TCP port 25123'
an IP address
38: resolve
for this particular domain
'an IP address'
'for this particular domain'
'In incoming'
37: discuss
'follow'
'In incoming'
'follow'
'Fix'
33: use
A4AF-4C7B1C9E648E.dll
34: use
msfsc.exe
'Fix'
msfsc.exe
35: exec
36: exec
A4AF-4C7B1C9E648E.dll
'*with the parameter k/r'
the malware
28: write
29: write
26: write
27: write
'Depending on its privileges'
'the files'
'in * or *'
'by creating a service'
'If the process is running with administrator privileges'
14: achieve
13: achieve
16: achieve
15: achieve
40: establish
the malware
by creating a service
persistence
'If an IP address is resolved for this particular domain'
39: establish
a connection on TCP port 25123
'If the process is running with administrator privileges'
'persistence'
'the process'
12: exec
'*with administrator privileges'
17: exec
19: write
18: write
25: write
23: write
20: write
24: write
22: write
'the dropper'
'in the C'
'msfsc.exe'
32: exec
58: exec
57: exec
31: exec
30: exec
'*C:\mainProcess.W'
'*+ files'
'*mfsg'
'If the dropper is executed with administrator privileges'
'After achieving persistance and dropping the executable'
msfc.dll
11: write
'This * ernest * application'
'%temp.exe'
'whose sole purpose'
'another application'
9: be
10: be
'whose sole purpose'
'another application'
'to delete the dropper'
'to delete the dropper'
'After The shellcode decrypted from the resource execution'
7: write
8: write
'%temp.exe'
'%temp.exe'
'From the resource executed'
5: decrypt
6: decrypt
3: decrypt
'The shellcode'
from the resource
from the resource execution
%%WO-24F8b60DF55F}.dll
'%%WO-24F8b60DF55F}.dll'
'The shellcode'
'From the resource'
'into the * folder'
'file'
3: write
4: exec
'*via Win32 API function ShellExecute'
the decrypted data (LZMA)
1: decrypt
2: decompress
the binary
in resource (XOR with a 128-byte , hardcoded key)
the decrypted data (LZMA)
the binary
'in resource (XOR with a 128-byte , hardcoded key)'