Yara script:

rule spyeye : banker

{

meta:

author = "Ben"

description = "SpyEye X.Y memory"

date = "2022-05-25"

version = "1.0 "

filetype = "memory"

strings:

$g = "bot\_version"

$h = "bot\_guid"

condition:

any of ($g,$h) and filesize >50000

}

Output:

