



Settings



Post



Christophe Tafani-Dereeper
@christophetd



Easiest way to detect this kind of behavior with Sysmon:

event_id=1
event_data.Company="Microsoft Corporation"
event_data.Description="Windows PowerShell"
event_data.Image != *powershell.exe

#sysmon #threat hunting

Computer name	Parent	Command line
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -windowstyle hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAd...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -windowstyle hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAd...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -windowstyle hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAd...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -windowstyle hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAd...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -windowstyle hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAd...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -windowstyle hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAd...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -w hidden -ep bypass -encodedCommand aB1lmgWkBuQJAdwTASBAtgBgQJYwB8CAcWlSAPPGAE1AGALghuQJAdwAmK4ZB...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -w hidden -ep bypass -encodedCommand aW4G51dy1vmpTfYQgc11z80YtLw51AC532KJ26G1lBnQkWhvD5d0Fkc3ByaW5wC2odW...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -w hidden -ep bypass -ec aW4G51dy1vmpTfYQgc11z80YtLw51AC532KJ26G1lBnQkWhvD5d0Fkc3ByaW5wC2odW...
DESKTOP-ABC	C:\Windows\Sysmon4\ushta.exe	"C:\Users\Public\Setup.exe" -w hidden -ep bypass -ec aW4G51dy1vmpTfYQgc11z80YtLw51AC532KJ26G1lBnQkWhvD5d0Fkc3ByaW5wC2odW...

1:54 PM · Aug 22, 2019

5 Reposts 1 Quote 37 Likes 3 Bookmarks



3



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