Settings

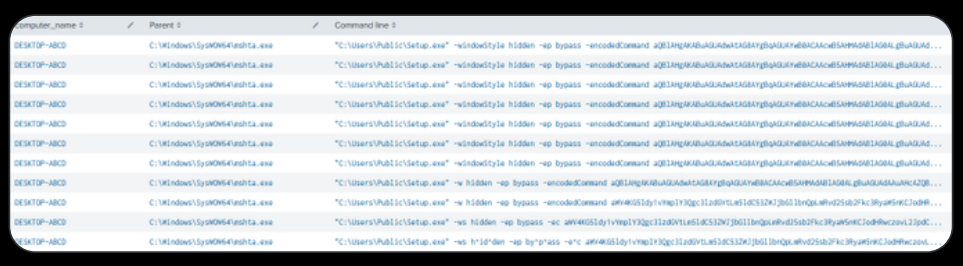
Post

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 #threathunting



1:54 PM · Aug 22, 2019

5 Reposts **1** Quote **37** Likes **3** Bookmarks