



Settings

← Post

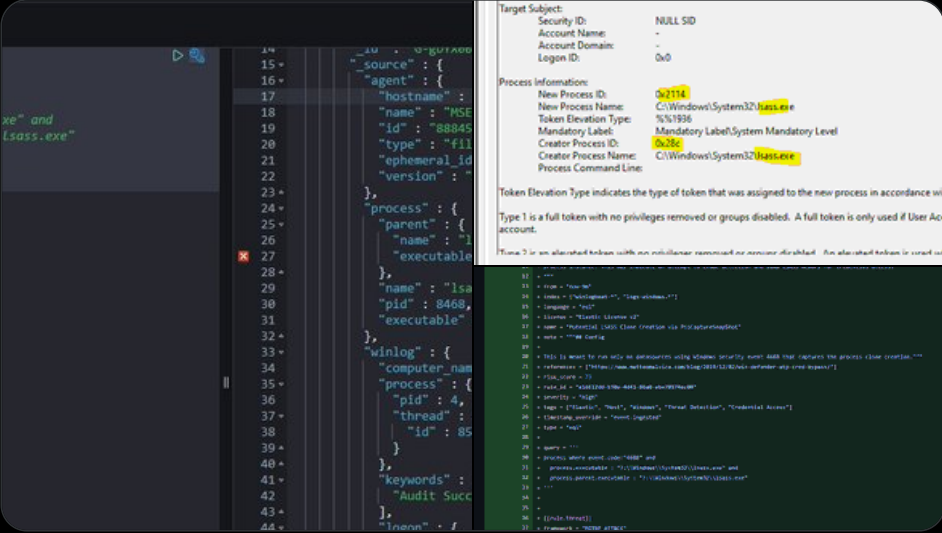


Samir
@SBousseaden



just added a detection for creating an LSASS clone to dump memory or alike using event 4688, more details in the PR:

github.com/elastic/detect...



Adam @Hexacorn · Jul 27, 2021

Replying to @BlackMatter23 @binaryzOne and 2 others

I guess it's PsInserProcess -> SeAuditProcessCreation ... -> 4688 and...
PsInserProcess is called before PsInserThread inside NtCreateUserProcess

1:08 PM · Nov 27, 2021

45 Reposts 1 Quote 180 Likes 35 Bookmarks



35



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