


←

Post



Stephan Berger

@malmoeb

...

1/ Nicely done, pointing out the renamed #Autolt tool in the alert below (see screenshot) 🧐.

The parameter "/Autolt3ExecuteScript" might be a good term for #hunting or for setting up monitoring for it when logging command lines 🤖

Or use @bartblaze AutoIT.yar repository [1] 📄

[14148] cmd.exe /c start ..\Microsoft\MicrosoftSecurity.exe /Autolt3ExecuteScript ..\Mi...

...

▼

⚙️

[58440] MicrosoftSecurity.exe /Autolt3ExecuteScript ..\Microsoft\Microsoft.a3x ...

...

▼

📄

File create MicrosoftSecurity.exe

...

▼

⚡

Renamed Autolt tool

...

■ ■ ■

Medium

●

Detected

●

Resolved (True alert)

File create Music.Ink

Malware

●

Prevented

...

▼

⚡

'WinLNK' malware was prevented

...

■ ■ ■

Informational

●

Prevented

●

New

11:01 PM · Jun 4, 2023 · 14.4K Views

22

Reposts

75

Likes

24

Bookmarks

💬

↺↻


❤️


🔖24

📤

New to X?

Sign up now to get your own personalized timeline!

 Sign up with Google

 Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.

⌂ Retry

[Terms of Service](#) [Privacy Policy](#) [Cookie Policy](#)
[Accessibility](#) [Ads info](#) [More ...](#) © 2024 X Corp.

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