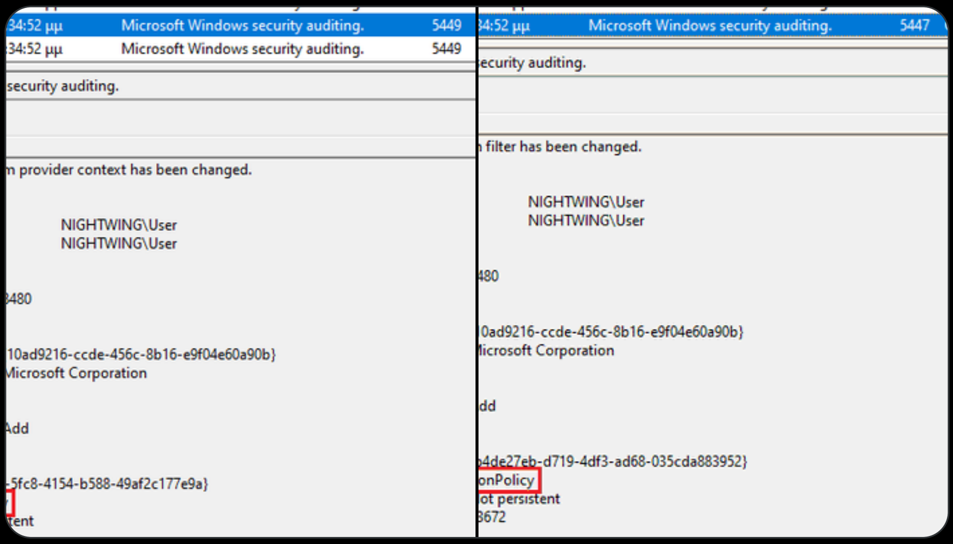
St0pp3r on X: "I recently looked into the creation of a rule for the #NoFilter #PrivilegeEscalation #hacktool by leveraging Event IDs 5447 &amp; 5449. The detection is based on the static value "RonPolicy" of the PolicyName variable in the code of the tool. https://t.co/W1OK8cXXBM #CyberSecurity https://t.co/8LLNMugXFu" / X - 02/11/2024 11:17 https://x.com/_st0pp3r_/status/1742203752361128162?s=20

Settings

Post

St0pp3r
@_st0pp3r_

I recently looked into the creation of a rule for the #NoFilter #PrivilegeEscalation #hacktool by leveraging Event IDs 5447 & 5449. The detection is based on the static value "RonPolicy" of the PolicyName variable in the code of the tool. github.com/deepinstinct/N... #CyberSecurity



```
34:52 μμ        Microsoft Windows security auditing.        5449
34:52 μμ        Microsoft Windows security auditing.        5449
security auditing.
n provider context has been changed.
        NIGHTWING\User
        NIGHTWING\User
3480
10ad9216-ccde-456c-8b16-e9f04e60a90b}
Microsoft Corporation
Add
-5fc8-4154-b588-49af2c177e9a}
tent
```

```
34:52 μμ        Microsoft Windows security auditing.        5447
ecurity auditing.
n filter has been changed.
        NIGHTWING\User
        NIGHTWING\User
480
0ad9216-ccde-456c-8b16-e9f04e60a90b}
licrosoft Corporation
dd
b4de27eb-d719-4df3-ad68-035cda883952}
onPolicy
ot persistent
3672
```

4:18 PM · Jan 2, 2024 · **269** Views

3 Reposts **8** Likes **3** Bookmarks

3

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