Sign in

olafhartong / **sysmon-modular** Public

Notifications Fork 589 Star 2.7k

Code Issues 32 Pull requests 20 Discussions Actions Projects Wiki

sysmon-modular / 11_file_create / **include_dotnet.xml**

16 lines (16 loc) · 1.51 KB

Code Blame Raw

```xml
<Sysmon schemaversion="4.30">
        <EventFiltering>
                <RuleGroup name="" groupRelation="or">
                        <FileCreate onmatch="include">
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                                <TargetFilename name="technique_id=T1218,technique_name=Office Sigr
                        </FileCreate>
                </RuleGroup>
        </EventFiltering>
</Sysmon>
```