WRITING GOOD SIGMA RULES

Thomas Patzke

2020-05-18

INTRODUCTION

MOTIVATION

This talk is not just about writing Sigma rules.

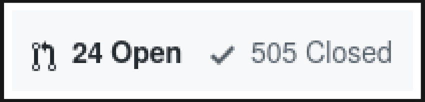
MOTIVATION

This talk is not just about writing Sigma rules.

...it's about writing *good* Sigma rules.

SIGMA RULE PULL REQUESTS

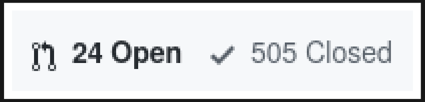
We get a lot of pull requests (PRs) - and we're happy about *every* one!



24 Open ✓ 505 Closed

SIGMA RULE PULL REQUESTS

We get a lot of pull requests (PRs) - and we're happy about *every* one!



24 Open ✓ 505 Closed

There's a lot of QA before a PR gets merged:

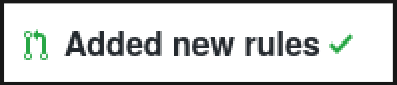
- Will there be false negatives?
- How likely are false positives?
- Is the detection efficient?
- But also: spelling, clean form, ...

TWO SHADES OF PULL REQUESTS

TWO SHADES OF PULL REQUESTS

The Sigma open source repository runs CI tests for each PR. This includes:

SHADE 1: CI TESTS PASS



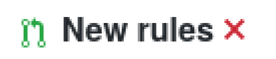
Added new rules ✓

SHADE 1: CI TESTS PASS

Added new rules ✓

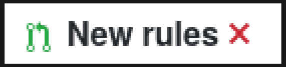
- Such a PRs meets the test requirements.
- It's likely that the QA process is finished quickly.
- It's more likely that the rule is merged quickly.

SHADE 2: CI TESTS FAIL



New rules ✗

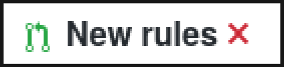
SHADE 2: CI TESTS FAIL



New rules ✗

- Some basic checks already fail for this PR.
- Such a PR likely causes more work.
- It's more likely that the merge will delay.

SHADE 2: CI TESTS FAIL


New rules ×

- Some basic checks already fail for this PR.
- Such a PR likely causes more work.
- It's more likely that the merge will delay.

Delays cause frustration at both sides: contributors and maintainers.

WHAT'S A GOOD SIGMA RULE?

There's a rule creation guide:

https://github.com/Neo23x0/sigma/wiki/Rule-Creation-Guide

WHAT'S A GOOD SIGMA RULE?

There's a rule creation guide: https://github.com/Neo23x0/sigma/wiki/Rule-Creation-Guide

It includes:

- a template
- Instructions for each attribute
- Common pitfalls

HANDS-ON

STARTING POINT

Lets take a look at CrackMapExec:

https://github.com/byt3bl33d3r/CrackMapExec

STARTING POINT

Lets take a look at CrackMapExec:
https://github.com/byt3bl33d3r/CrackMapExec

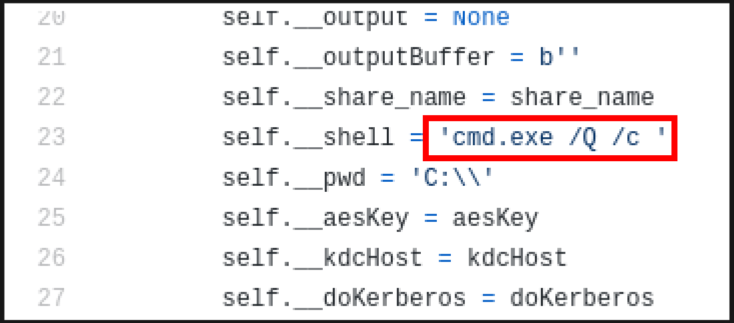
This tool contains some very distinctive command lines.

CRACKMAPEXEC: WMI EXECUTION

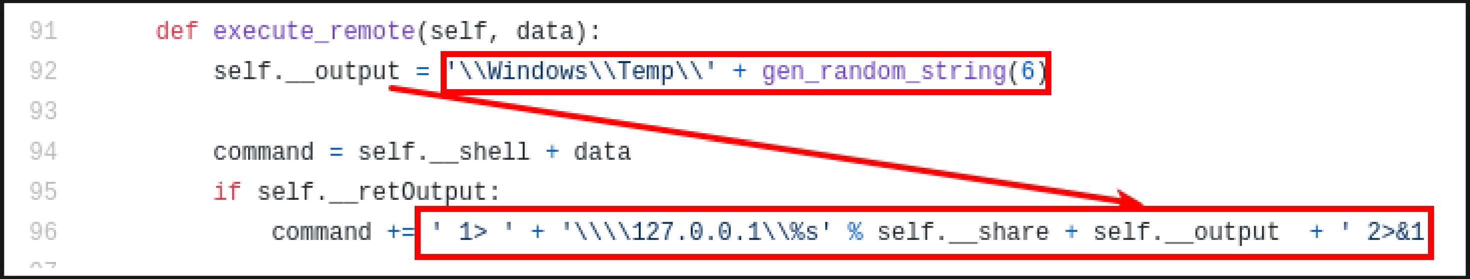
Link to file:

https://github.com/byt3bl33d3r/CrackMapExec/blob/ma

INTERESTING LOCATIONS



```
        self.__output = None
        self.__outputBuffer = b''
        self.__share_name = share_name
        self.__shell = 'cmd.exe /Q /c '
        self.__pwd = 'C:\\'
        self.__aesKey = aesKey
        self.__kdcHost = kdcHost
        self.__doKerberos = doKerberos
```



```
    def execute_remote(self, data):
        self.__output = '\\Windows\\Temp\\' + gen_random_string(6)

        command = self.__shell + data
        if self.__retOutput:
            command += ' 1> ' + '\\\\127.0.0.1\\%s' % self.__share + self.__output  + ' 2>&1
```

DEVELOPING A SIGNATURE

The command line looks as follows:

- It starts with: `cmd.exe /Q /c`
- It contains: `1> \\127.0.0.1\\`
- Which is followed by: `\\Windows\\Temp\\` followed by some random characters.
- It ends with: 2>&1

LET'S WRITE THE SIGMA RULE!

1. Copy & paste the template
2. Write the rule
3. Test the rule
4. Contribute!

TEST THE RULE

- Run Sigma converter (quick)
- Run CI tests (complete)

CONTRIBUTE OR PUBLISH

- To the Sigma main repository: https://github.com/Neo23x0/sigma

CONTRIBUTE OR PUBLISH

- To the Sigma main repository: https://github.com/Neo23x0/sigma
- Threat Bounty: https://my.socprime.com/en/tdm-developers/

CONTRIBUTE OR PUBLISH

- To the Sigma main repository: https://github.com/Neo23x0/sigma
- Threat Bounty: https://my.socprime.com/en/tdm-developers/
- Perhaps offensive tool developers are happy about directly providing signatures for their released tools in *their* project repositories?

SUMMARY

WRITING A GOOD SIGMA RULE

- Use the template!
- Keep the title short, omit obvious
- Provide context ad tags, references and descriptions
- Try to omit regular expressions, they are expensive
- Minimize usage of wildcards
- Do testing!

QUESTIONS? CONTACT US!

GitHub Issues:
https://github.com/Neo23x0/sigma/issues/new

Or directly:

E-Mail: thomas@patzke.org

My Twitter: https://twitter.com/blubbfiction

Florians Twitter: https://twitter.com/cyb3rops