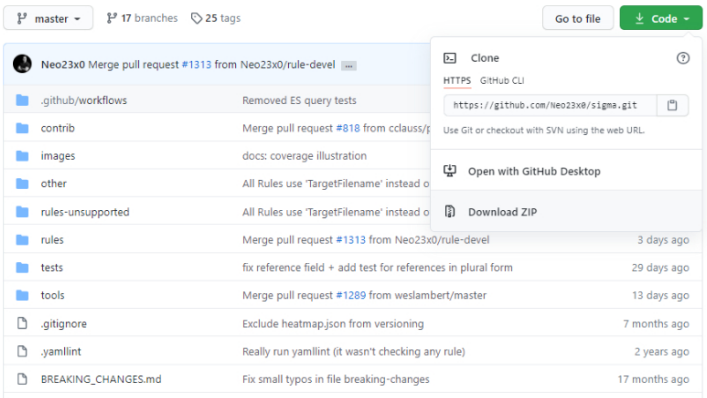
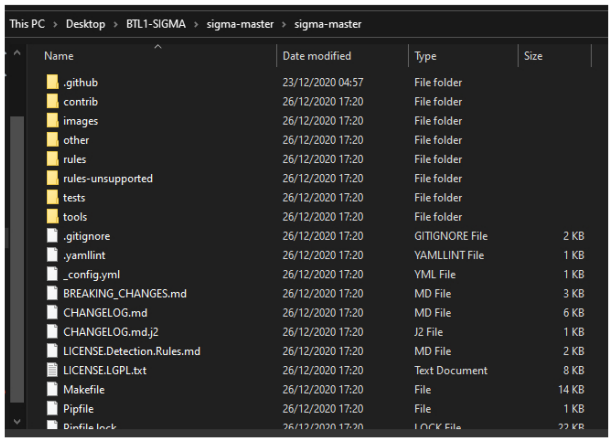
Activity) Writing Sigma Rules

In this activity you're going to be taking a look at some Sigma rules and writing your own by editing a pre-built rule. The purpose of this activity is to get you familiar with a vendor-agnostic detection format that can be applied to major SIEM providers, but also to develop your ability to think logically about detections.

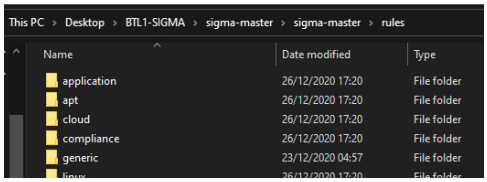
First, you'll need to go download the Sigma master ZIP file from the Github:

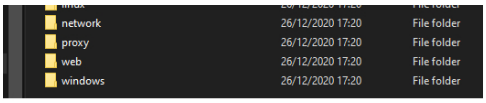


Once you have the .ZIP file we need to extract the contents. To make things easier create a folder on your Desktop called 'BTL1-SIGMA', move the downloaded ZIP file to this folder, then extract it.

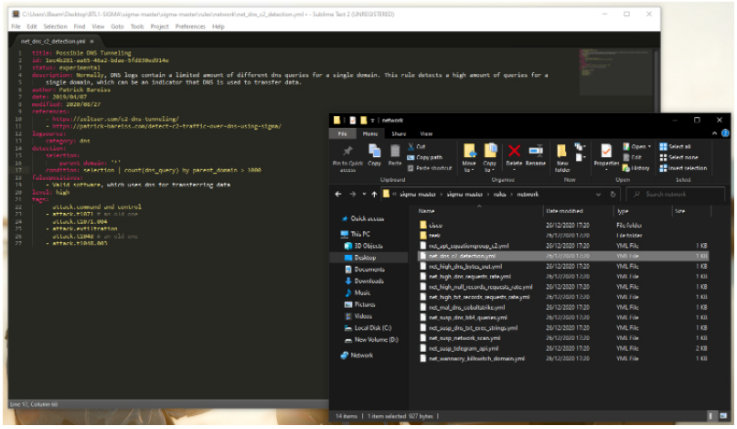


Open the 'rules' folder – we're presented with a number of sub-folders that contain some basic rules:





Now go into the 'network folder' and then open 'net_dns_c2_detection.yml' in Sublime Text 2 (or your text editor of choice):



Before we start customing this rule to suit our own needs, let's recap exactly what this rule is doing and how it's formatted. Take note of the different rows explained below, as you'll be editing some of these very soon!

```
title: Possible DNS Tunneling
id: 1ec4b281-aa65-46a2-bdae-5fd830ed914e
status: experimental
description: Normally, DNS logs contain a limited amount of different dns queries for a single domain. This rule detects a high amount of queries for a
    single domain, which can be an indicator that DNS is used to transfer data.
author: Patrick Bareiss
date: 2019/04/07
modified: 2020/08/27
references:
    - https://zeltser.com/c2-dns-tunneling/
    - https://patrick-bareiss.com/detect-c2-traffic-over-dns-using-sigma/
logsource:
    category: dns
detection:
    selection:
        parent_domain: '*'
    condition: selection | count(dns_query) by parent_domain > 1000
falsepositives:
    - Valid software, which uses dns for transferring data
level: high
tags:
    - attack.command_and_control
    - attack.t1071 # an old one
    - attack.t1071.004
    - attack.exfiltration
    - attack.t1048 # an old one
    - attack.t1048.003
```

1. **title** is a custom descriptive value that is used to provide a very brief explanation of what the rule is looking for.
2. **id** is used as a unique identifier for this rule.
3. **status** is a custom descriptive value used to explain the state of the rule. Some examples could include 'incomplete', 'experimental', or 'production'.
4. **description** is a custom descriptive value used to provide a more detailed explanation of what the rule is trying to detect and how.
5. See above.
6. **author** is a custom value used to hold the author(s) of this SIGMA rule.
7. **date** is a custom value used to hold the date the rule was first created.
8. **modified** is a custom value used to hold the date when the rule was last edited by an author.
9. **references** is a custom list that holds URLs that help to explain what the rule is trying to detect
10. see above
11. see above
12. **logsource** is used to explain what logs are required in the SIEM for the rule to function
13. the **logsource category** is dns, showing that the security team will need to be pulling dns logs into their SIEM for the rule to work
14. **detection** explains the logic behind the rule including conditions that, when met, can generate an alert.
15. **selection** states that something must be selected from the DNS logs. In this case it's the parent domain (or root domain, such as Google.com).
16. **parent_domain** states the log field that should be selected. The * asterisk symbol represents a 'wildcard' meaning that any value can be used. This means that ANY domain should be selected.
17. **condition** states the actual detection logic. For this rule it will retrieve all parent_domain values and count the number of queries to that domain. If the count is over 1000 (> 1000 meaning greater than 1000) then it will alert.
18. **falsepositives** is a custom list that states how false positives could occur.
19. **falsepositives 2** – The author explains that legitimate software that uses dns to transfer data would generate an alert, even though it is not malicious activity.
20. **level** is a custom descriptive value that in this rule appears to be stating how urgent this alert should be.
21. **tags** is a custom list that includes different MITRE ATT&CK techniques that can be detected using this rule.

So, we know that this rule is used to detect potential DNS tunneling for command-and-control communication by looking for a large number of queries to domains, and will alert when 1001 or more requests have been observed by looking at DNS logs.

Now it's your turn to make some changes, allowing us to detect some specific activity. Read the intelligence briefing below and try to make changes to this existing rule file to reflect the information provided.

Intelligence Briefing

We've recently observed a new type of malware that we have named 'TRANSPORTER' which uses DNS tunneling to provide a command-and-control channel across the internet, allowing an attacker to send commands to infected systems. As DNS traffic is extremely common in environments this traffic blends in and does not immediately look suspicious. DNS packets contain many fields and headers in which data can be concealed.

At the time of writing, we have only observed one domain name that is being used to send and receive C2 traffic, which we have included below. Speaking with one victim we observed that their SIEM did not detect this activity as they were not monitoring for excessive DNS queries to domains.

Domain Name: redhunt.net
Average Number of Requests: 500
MITRE ATT&CK Techniques Used: T1071.004 (Application Layer Protocol: DNS)

Tips

- You can remove the 'id' and 'modified' lines from the existing rule as they are not required.
- Use the 'title' and 'description' lines to include information from the above intel briefing.
- Consider the average number of requests, we should alert on something that is lower than this to catch any infections where the traffic count falls below this average.

Previous Topic

Mark Complete

Back to Lesson