badpanda Configuration File Manual

blueintel

October 1, 2020

badpanda Configuration File

The badpanda configuration file is named ”badpanda.config” and stores the keywords and domain names that will be monitored for your organization. The file is a plain text file that can be edited with any text editor (not word processor). Please DO NOT save the file as a 16-bit Unicode file. The file must be saved as UTF-8 or ASCII. A minimalistic example of a badpanda.config file might look like this:

```
[org]
Widgets ltd.

[keywords]
fantastic
gadgets

[domains]
widgets.com
gadgets.com
```

Each section of the badpanda.config file is described below.

Configuration File Sections

The badpanda.config file is divided into sections. Each section has a name surrounded by square brackets (e.g. [domains]). Values for a section are listed one per line. All names and values should be lowercase only. Supported sections are:

- org
- contacts
- domains
- keywords

Most sections support tags that further categorize the information. Tags are designated by a dot(.). For example [domains.email] designates section ”domain” tagged as ”email”. Supported tags and subtags are listed in the documentation below. Tagging your information is the primary way to reduce false positives and reduce unnecessary processing.

Comments may begin anywhere on a line. Comments begin with ”;” and continue to the end of the line.

[org] Section

The [org] section is a free-form section used to describe your organization. No tags are supported for the [org] section. You only need to specify the name of your organization here.

Example:

```
[org]
widgets ltd.
```

[contacts] Section

The [contacts] section is a list of email addresses to which technical reports will be sent. Each email address must be on its own line. The advantage of placing email addresses in the configuration file is that you do not need to create an organization user for every destination that should receive technical emails. This is commonly used to send to mailboxes that are processed using automated tools.

Example:

```
[org]
widgets ltd.

[contacts]
threatintel@example.com
bob@example.com
```

[domains] Section

The [domains] section lists domains associated with your organization. Follow these guidelines to avoid many false positives.

- Do not list subdomains (hostnames) of your domain. The blueintel tools will strip them off anyway so that all hits on your domain name may be found. For example, you should list ”example.com” but not ”www.example.com”. ”www.example.com” is redundant because ”www” will be stripped before processing.
- Do not list the same domain with multiple top-level domains. For example, do not list both ”example.com” and ”example.net”. The top-level domains ”.com” and ”.net” are stripped before processing because they are not used during the matching process.
- Do not list a domain if it is less than four characters long as it will be ignored. Experience has found that domains of less than four characters result in too many false positives to be useful.
- Do not list a domain if it is a common word such as ”place” since such domains result in too many false positives to be useful. An alternative approach using keywords to monitor common words will be described in the [keywords] section below.

Example:

```
[org]
widgets ltd

[contacts]
threatintel@example.com
bob@example.com

[domains]
widgets.com
buywidgets.com
info-widgets.info
```

[keywords] Section

There can actually be more than one [keywords] section, however the easiest way to use keywords is to specify just one. This technique will work for most organizations and is the recommended way to use keywords when just starting out. The default behavior for the [keywords] section is that two or more keywords in the [keywords] section must match the domain being examined for a successful match.

Example:

```
[org]
widgets ltd

[keywords]
widgets
acme
international
```

In the example above, two or more keywords must match the examined domain for that domain to be included in the list of suspicious domains. If your organization has a domain name that is causing a lot of false positives, follow these steps to reduce them:

1. Remove the domain from the [domains] section.
2. Remove the top level domain from the domain name and add the domain to the [keywords] section (e.g. add "acme" to the keywords, not "acme.com").
3. Add additional keywords to the [keywords] section that are related to your organization.

For example, if "acme.com" in the [domains] section causes lots of false positives, remove it from the the list of domains, add "acme" to the list of keywords, and add additional keywords such as "widgets" or "international". Only when two or more of these keywords match will the domain be reported.

If these steps are not sufficient to reduce the number of false positives, please refer to the section below on adding tags to keywords.

keywords With Tags

You may need to add tags to keywords and a [keywords.conditions] section to reduce the number of false positives. This usually occurs when domain names and/or two or more of the keywords are common words. bimeta supports using multiple keywords sections with tags and a YARA-like conditional language to specify more complex criteria for a successful match.

Keywords may be divided into tagged groups such that rules can be specified that one or more keywords must be matched or excluded in one or more tagged groups.

[keywords.conditions] section

The [keywords.conditions] section is a special section that contains rules that specify how sets of keywords should be matched. The conditions are similar to those used by YARA. Conditions specify how many keywords in each tagged section must be matched for the candidate domain to match. For example, if you have two tagged keyword sections [keywords.basic] and [keywords.highFidelity], you may want any candidate domains that include just one keyword in [keywords.highFidelity] to be considered a match but require that two keywords in [keywords.basic] be matched if the candidate domain does not contain a keyword in [keywords.highFidelity]. This is accomplished with the following condition in [keywords.conditions]:

```
1 in $keywords.highFidelity or 2 in $keywords.basic
```

Conditions must follow these rules:

- Conditions may contain multiple expressions separated by "and" or "or".

- Each expression is a number followed by the word ”in” followed by the name of the keyword section preceded by a ”$” sign. For example, you must refer to [keywords.basic] as ”$keywords.basic”.

- The number in the expression is a minimum number so a match will be found if that number or more keywords are in the candidate domain. In the previous example, a candidate domain matches if 1 or more keywords in [keywords.highFidelity] or 2 or more keywords in [keywords.basic] are found in the domain.

- The ”negative” tag is a special tag used to specify keywords that when matched will filter out domains containing any of those keywords.

- Use ”none in $keywords.negative” in conditions to filter out domains with negative keywords. Negative keywords are useful when many false positives are reported. For example, ”author” could be added to the list of negative keywords to avoid false positives for the domain ”thor.com”.

- Conditions must be on a single line.

- Multiple conditions may be specified. If any of the conditions match the domain, the domain is added to the report.

- Parentheses may be used to group expressions to specify precedence.

- Only use conditions if you are really receiving too many false positives because custom conditions may have an impact on system performance.

Example of using three different keyword sections:

```
none in $keywords.negative and (1 in $keywords.highFidelity or 2 in $keywords.basic)
```

This condition will match all domains that contain one or more keywords in [keywords.highFidelity] or two or more keywords in [keywords.basic] and no keywords in [keywords.negative] match the domain.

Configuration Example 1

This is a complete example showing a typical configuration.

```
; org section identifies your organization
[org]
Widgets Inc.

; contacts are email addresses, one per line
[contacts]
threatintel@example.com

; Basic keywords used by org. The conditions section
; states that 2 or more of these must match for the
; domain to be reported.
[keywords]
animal
vegetable
mineral

; The conditions section states that one or more of these
; keywords must match for the domain to be reported.
[keywords.highFidelity]
widget

; If any keywords in this section match, then the domain
; will not be reported.
[keywords.negative]
gadget

; List of domains, one per line, no host names or subdomains
; and no repeats of domains where the only difference between
; them is the top level domain (e.g. widgets.com is listed so
; widgets.net is not).
[domains]
widgets.com
mywidgets.com
widget-blog.com
```

Configuration Example 2

This is a complete example showing all sections with comments and including [keywords.conditions].

```
; org section identifies your organization
[org]
Widgets Inc.

; contacts are email addresses, one per line
[contacts]
threatintel@example.com

; Basic keywords used by org. The conditions section
; states that 2 or more of these must match for the
; domain to be reported.
[keywords.basic]
animal
vegetable
mineral

; The conditions section states that one or more of
; these keywords must match for the domain to be
; reported.
[keywords.highFidelity]
widget

; If any keywords in this section match, then the domain
; will not be reported.
[keywords.negative]
gadget

; This condition will match all domains that contain one
; or more keywords in [keywords.highFidelity] or two or
; more keywords in [keywords.basic] and no keywords in
; [keywords.negative] match the domain.
[keywords.conditions]
none in $keyword.negative and (1 in $keywords.highFidelity or 2 in $keywords.basic)

; List of domains, one per line, no host names or subdomains
; and no repeats of domains where the only difference between
; them is the top level domain (e.g. widgets.com is listed so
; widgets.net is not).
[domains]
widgets.com
mywidgets.com
widget-blog.com
```