BISHOP FOX

Laika BOSS

BY LOCKHEED MARTIN

November 3, 2016

Introduction

WHO AM I?

Matthew Gleason

Senior Security Analyst

Agenda

LAIKA BOSS

- **Product Overview**
- **Demonstration**
- **Major Use Cases**
- **Product Considerations**

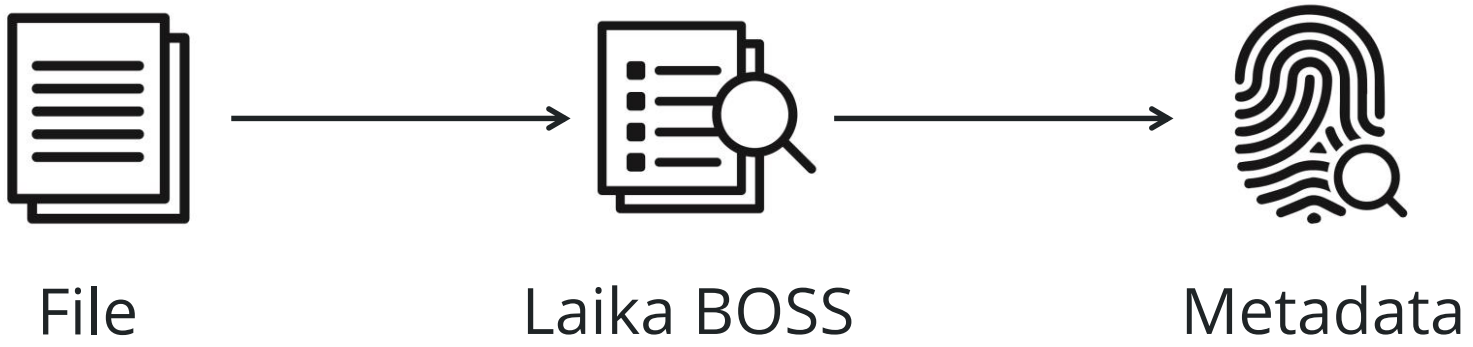
File

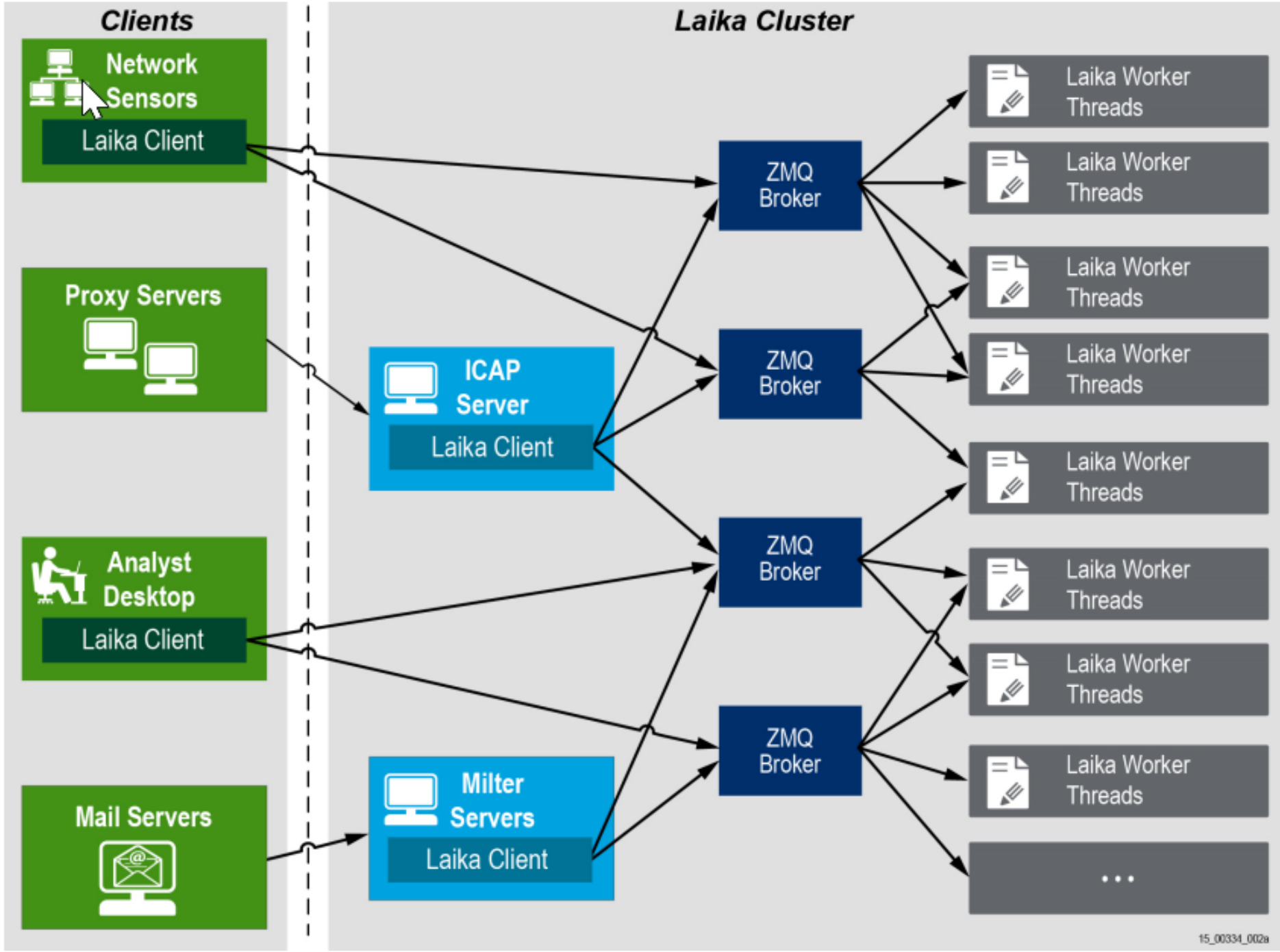
PRODUCT OVERVIEW

WHAT IS LAIKA BOSS?

Simplified View

MAYBE A LITTLE OVERSIMPLIFIED




Clients
Laika Cluster
Network Sensors
Laika Client
Proxy Servers
ICAP Server
Laika Client
Analyst Desktop
Laika Client
Mail Servers
Milter Servers
Laika Client
ZMQ Broker
ZMQ Broker
ZMQ Broker
ZMQ Broker
Laika Worker Threads
Laika Worker Threads
Laika Worker Threads
Laika Worker Threads
Laika Worker Threads
Laika Worker Threads
Laika Worker Threads
Laika Worker Threads
...
15_00334_002a

Associated Technologies

OTHER THINGS WE NEED TO KNOW ABOUT

Associated Technology	Reason
YARA	Custom file signatures • Know how to interpret files • Creation of signatures
ClamAV	Standard Antivirus • Detection of malicious files
ZeroMQ	Messaging Queue • Asynchronous worker design
Fluentd	Logging

YARA

RULES AND SIGNATURES

- Tool designed to help **identify and classify malware** using descriptions of patterns within the files.

- Each of these patterns, called a **rule**, is **designed to identify** a class of file.

- Standard rulesets are available all over the Internet for **detection of known viruses, exploit kits, web shells, etc.**

YARA

RULES AND SIGNATURES

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

YARA

RULES AND SIGNATURES

```
rule php_in_image
{
    meta:
        author      = "Vlad https://github.com/vlad-s"
        date        = "2016/07/18"
        description = "Finds image files w/ PHP code in images"
    strings:
        $gif = /^GIF8[79]a/
        $jfif = { ff d8 ff e? 00 10 4a 46 49 46 }
        $png = { 89 50 4e 47 0d 0a 1a 0a }

        $php_tag = "<?php"
    condition:
        (($gif at 0) or
        ($jfif at 0) or
        ($png at 0)) and

        $php_tag
}
```

ClamAV

OPEN-SOURCE ANTIVIRUS

- Open source antivirus engine for signature-based virus detection.
- Standard AV seen on most Unix-based OSes

ZeroMQ

SCALABILITY

- A lightweight message queue meant to assist for communication between processes.

- Open-source and cross platform.

Fluentd

LOGGING

- Open-source data collector
- Simplifies logging

Laika BOSS

RULES AND SIGNATURES

- Like YARA, Laika BOSS uses rules to interpret files.
- These rules tell Laika how to further process the object as well as recognize the type.

```
rule type_is_email
{
    meta:
        scan_modules = "META_EMAIL EXPLODE_EMAIL"
        file_type = "eml"
    strings:
        $from = "From "
        $received = "\x0aReceived:"
        $return = "\x0aReturn-Path:"
    condition:
        (not ext_sourceModule contains "EXPLODE_EMAIL") and
        (($from at 0) or
        ($received in (0 .. 2048)) or
        ($return in (0 .. 2048)))
}
```

Laika BOSS

MODULES

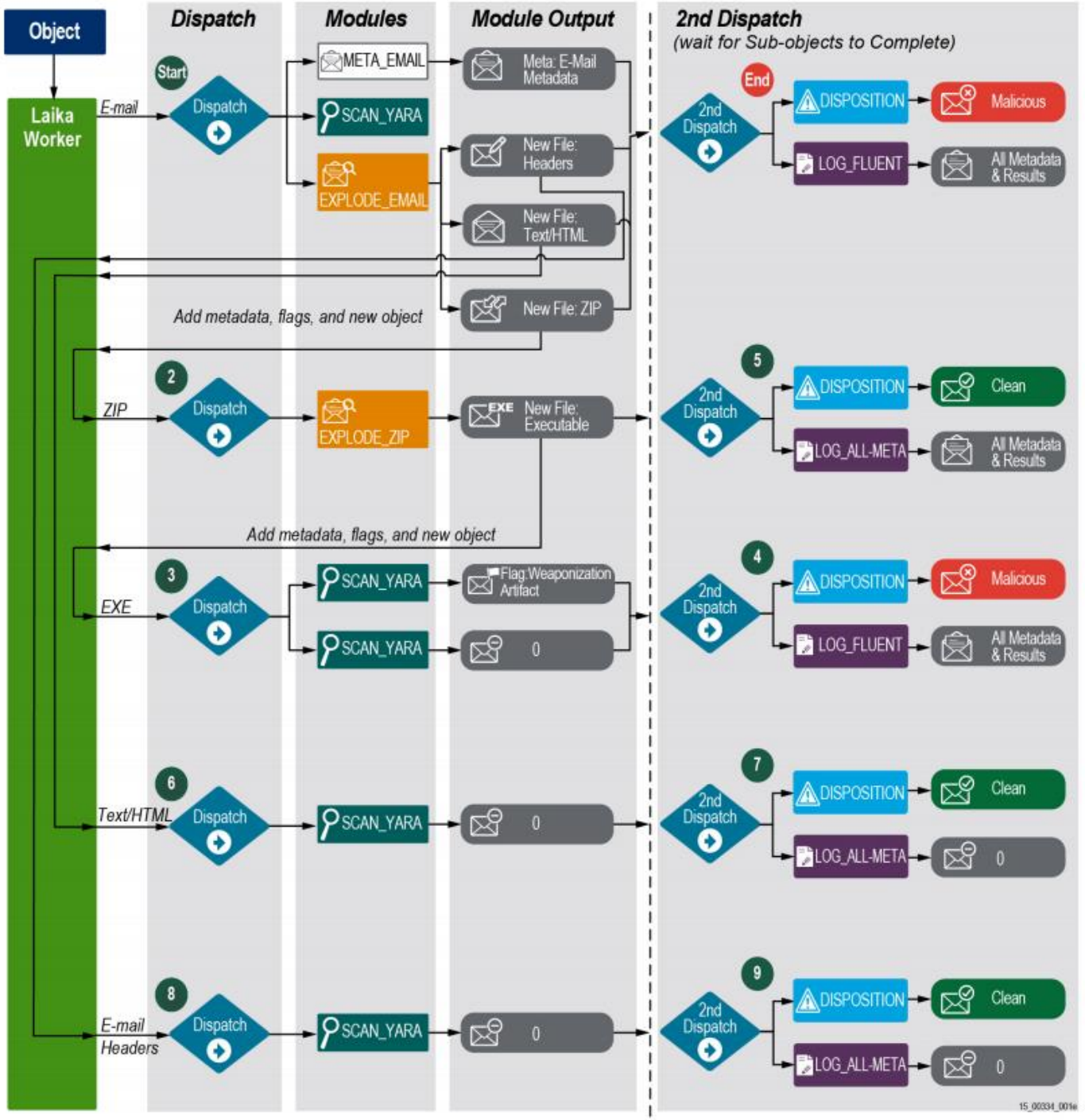
Unlike YARA, Laika BOSS can use modules.

- Written in Python.
- Extract Metadata and extract other objects for more processing.
- Custom modules can be written.

```
rule type_is_email
{
    meta:
        scan_modules = "META_EMAIL EXPLODE_EMAIL"
        file_type = "eml"
    strings:
        $from = "From "
        $received = "\x0aReceived:"
        $return = "\x0aReturn-Path:"
    condition:
        (not ext_sourceModule contains "EXPLODE_EMAIL") and
        (($from at 0) or
        ($received in (0 .. 2048)) or
        ($return in (0 .. 2048)))
}
```

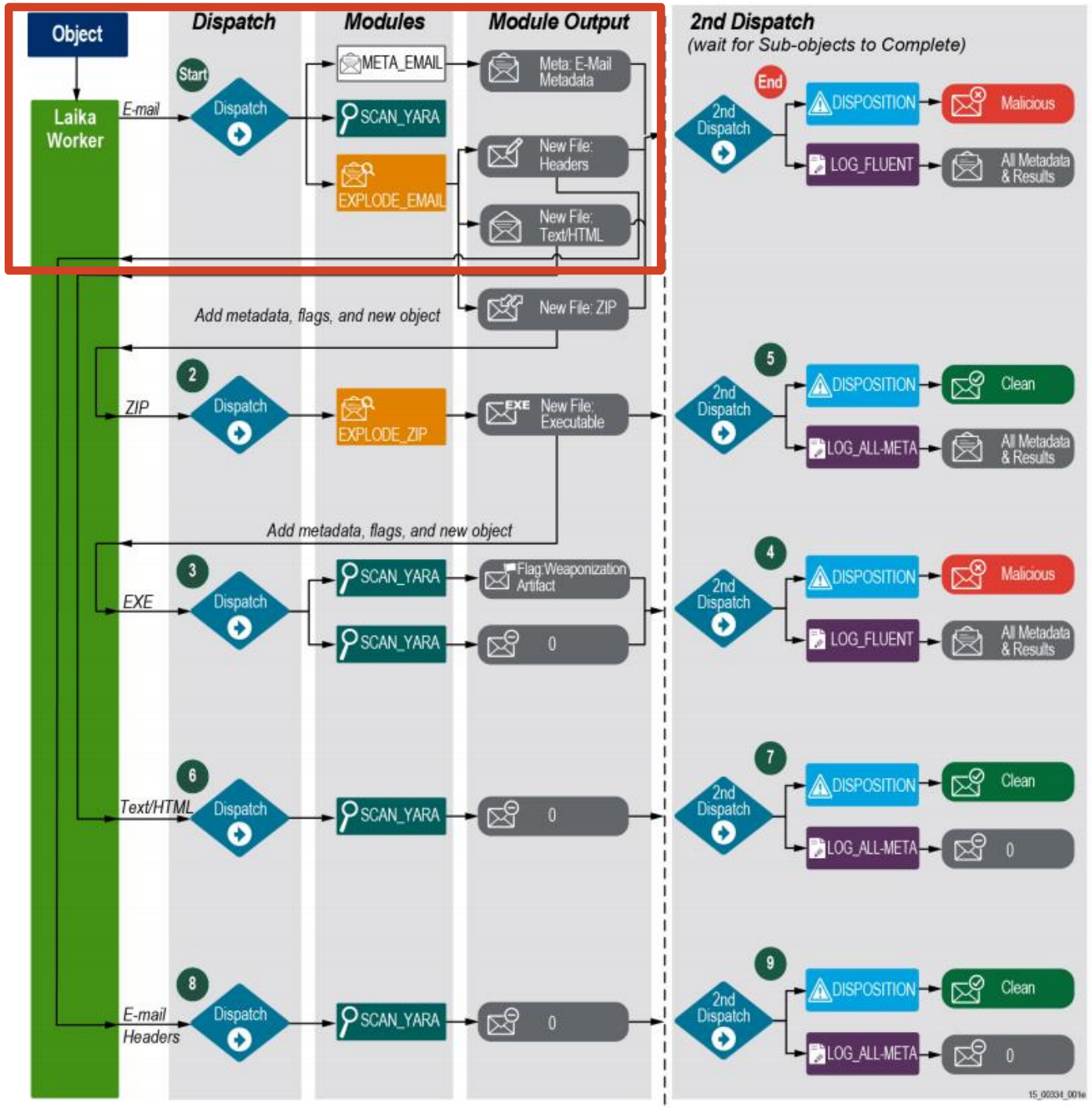
Laika BOSS

READING AN EMAIL



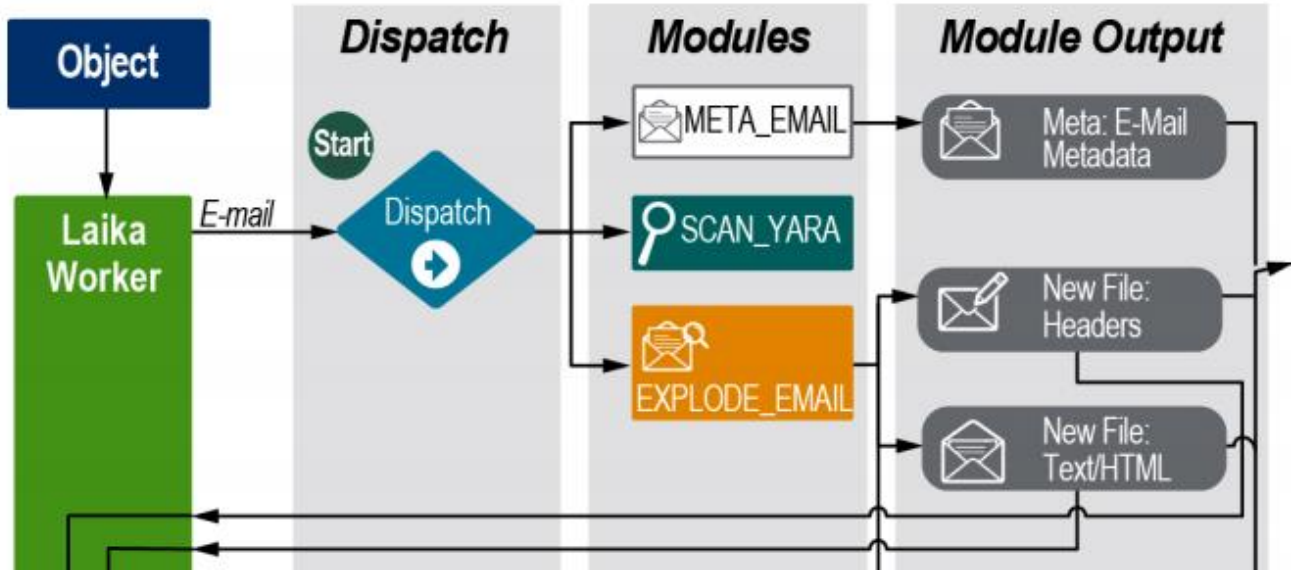
Laika BOSS

READING AN EMAIL



Laika BOSS

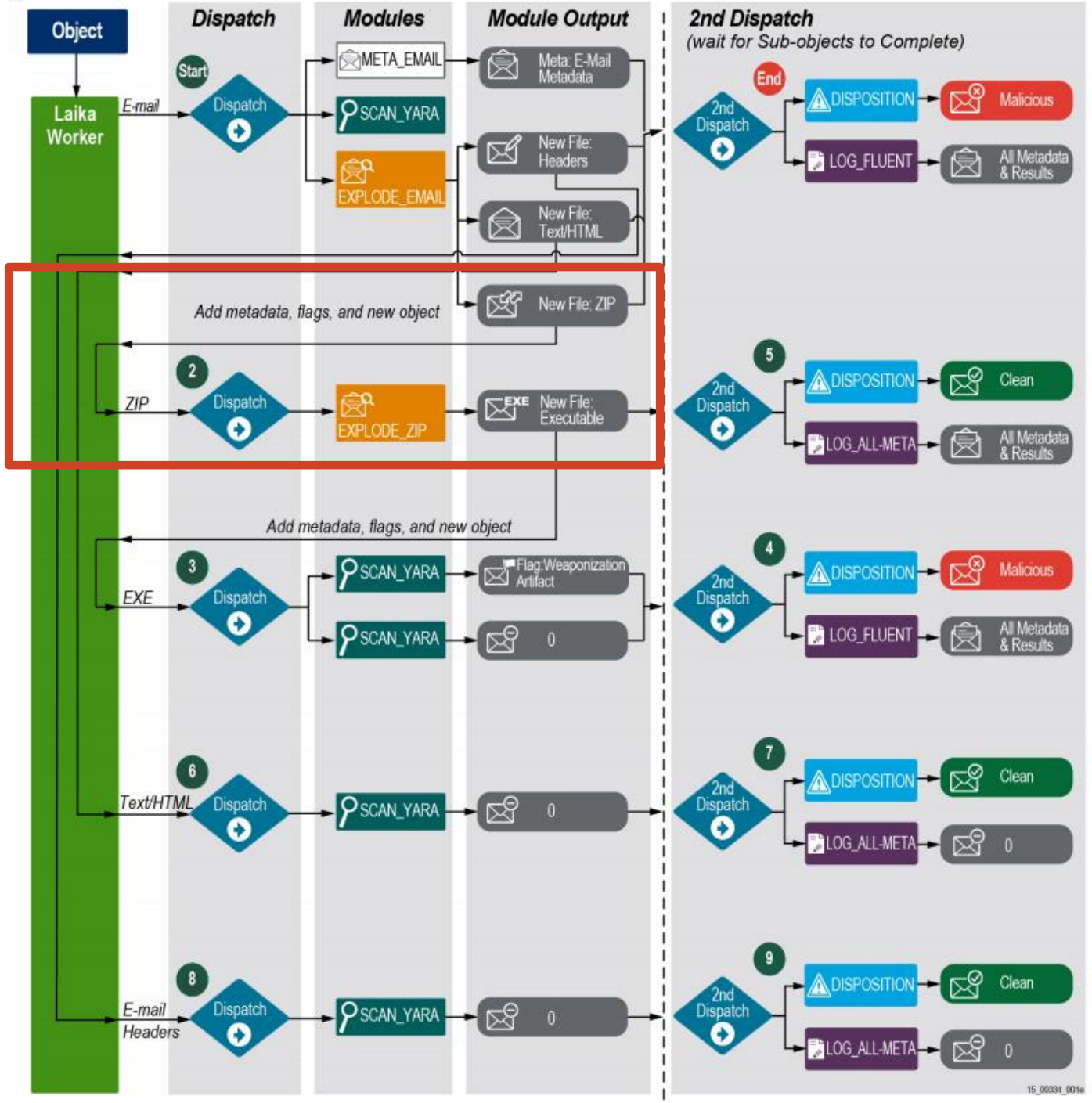
READING AN EMAIL




```
rule type_is_email
{
    meta:
        scan_modules = "META_EMAIL EXPLODE_EMAIL"
        file_type = "eml"
    strings:
        $from = "From "
        $received = "\x0aReceived:"
        $return = "\x0aReturn-Path:"
    condition:
        (not ext_sourceModule contains "EXPLODE_EMAIL") and
        (($from at 0) or
        ($received in (0 .. 2048)) or
        ($return in (0 .. 2048)))
}
```

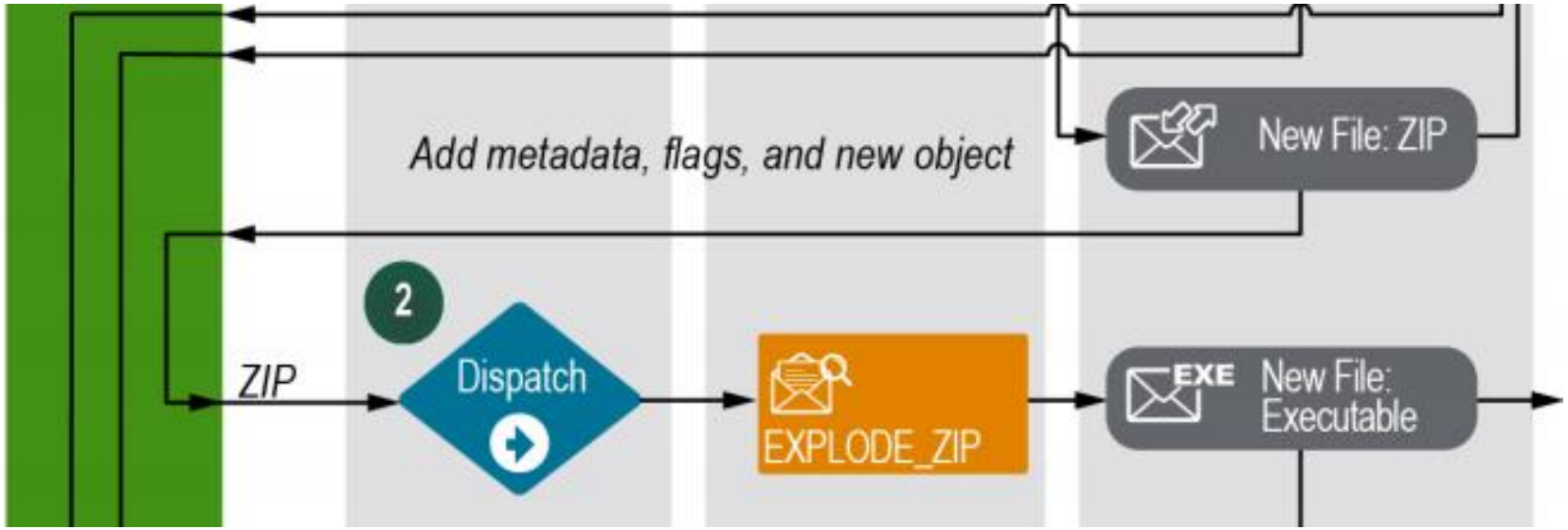
Laika BOSS

READING AN EMAIL



Laika BOSS

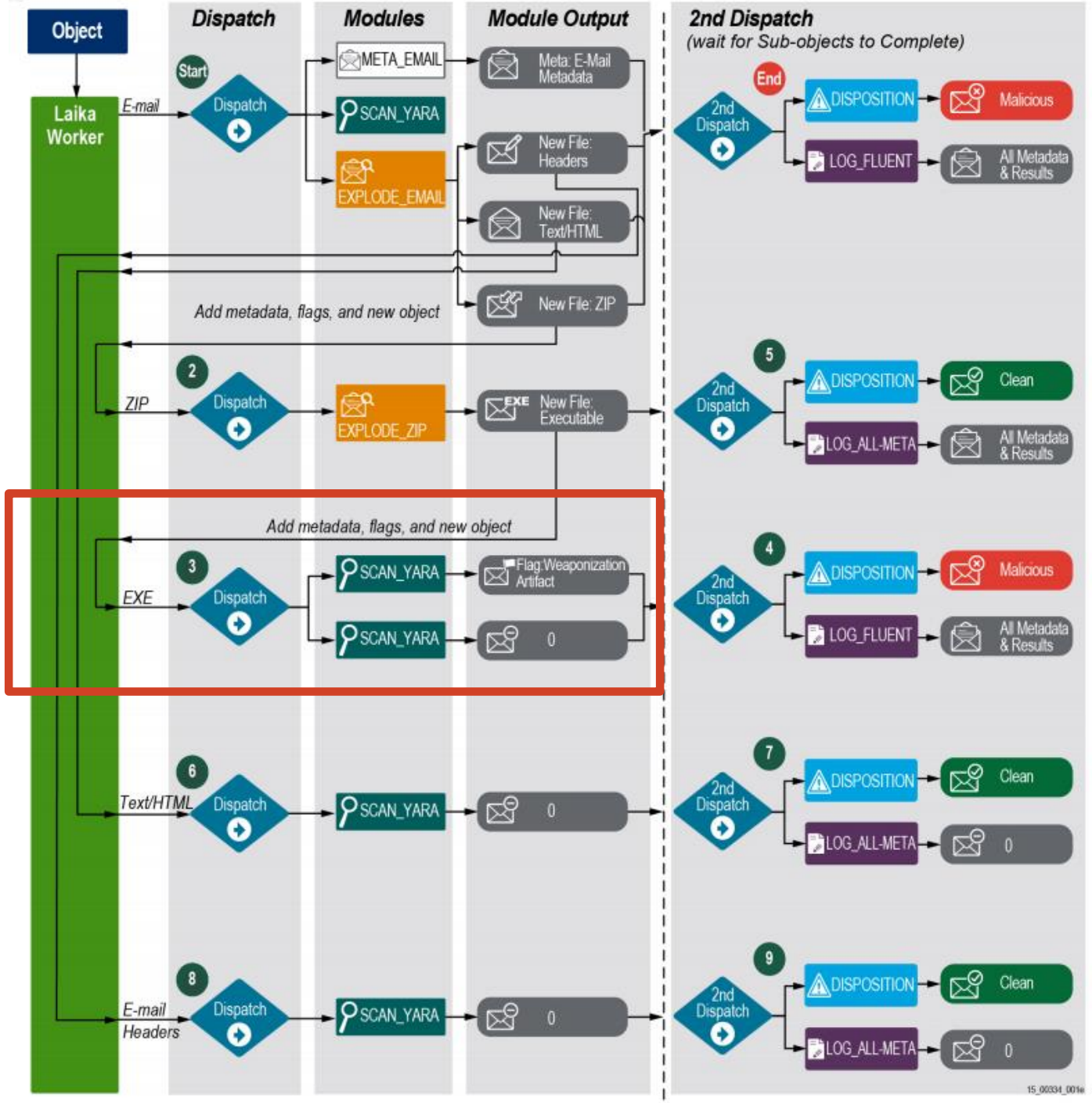
READING AN EMAIL




```
rule type_is_zip
{
    meta:
        scan_modules = "EXPLODE_ZIP(filelimit=1000)"
        file_type = "zip"
    condition:
        uint32(0) == 0x04034b50 and not uint32(4) == 0x00060014
}
```

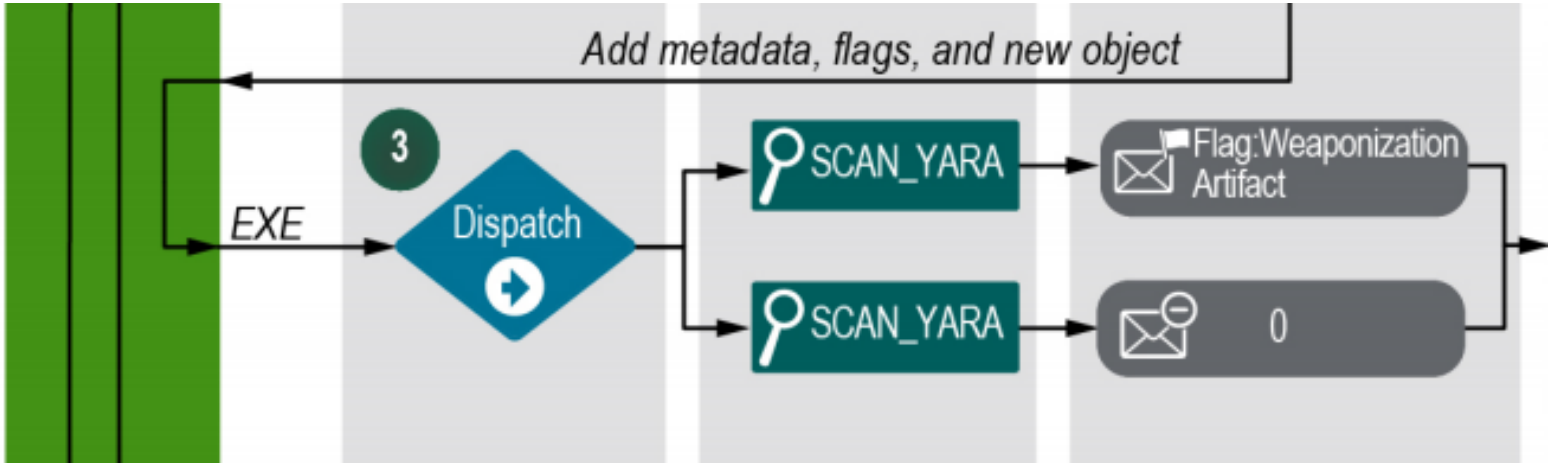
Laika BOSS

READING AN EMAIL



Laika BOSS

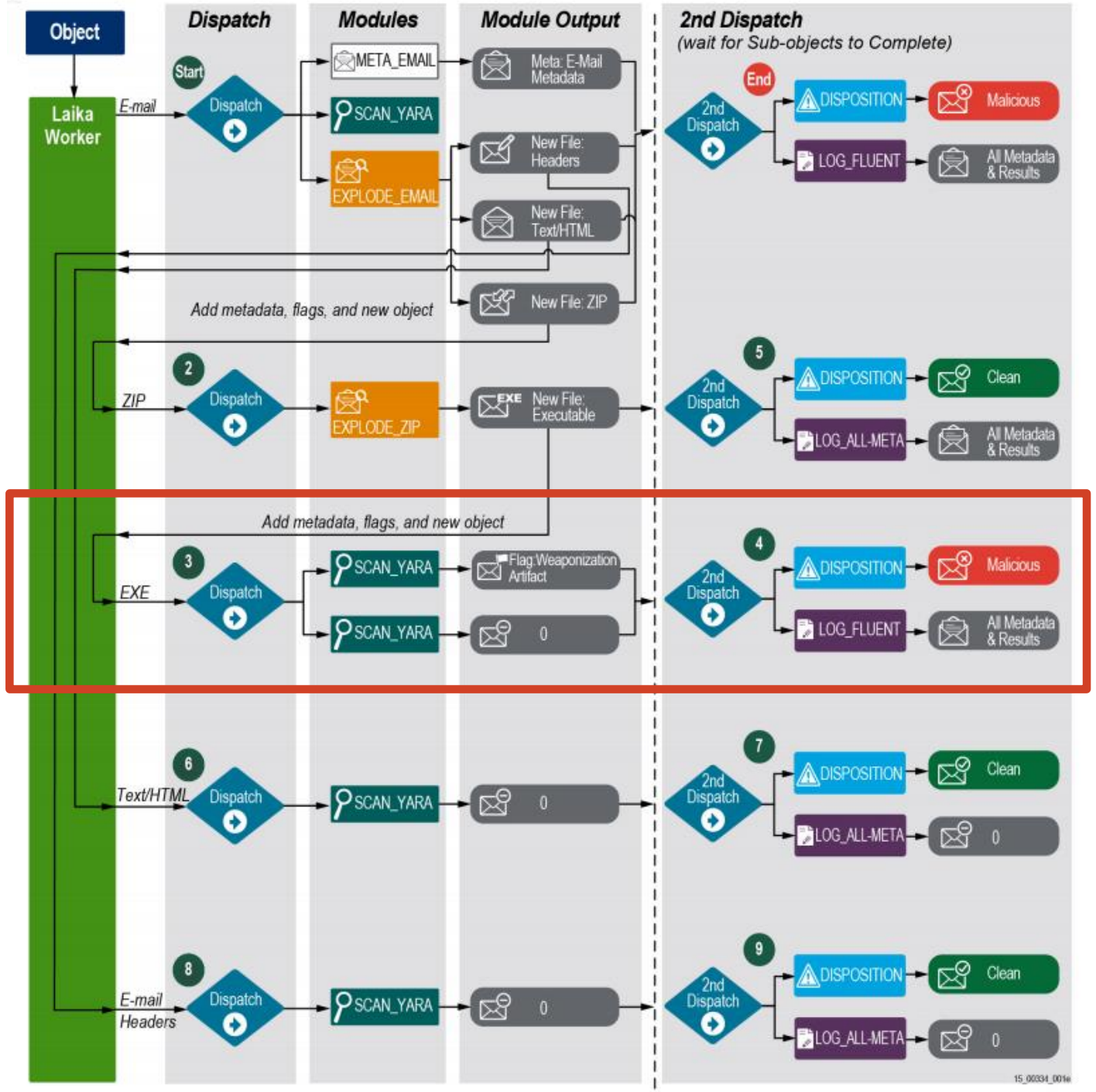
READING AN EMAIL




```
rule exe_in_zip
{
    meta:
        flags = "misc_exe_in_zip"
    condition:
        ext_sourceModule contains "EXPLODE_ZIP" and
        type_is_mz
}
```

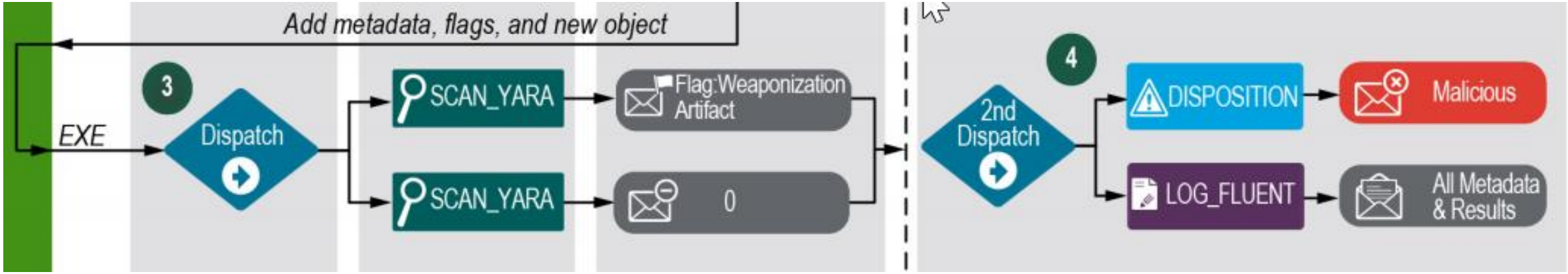
Laika BOSS

READING AN EMAIL



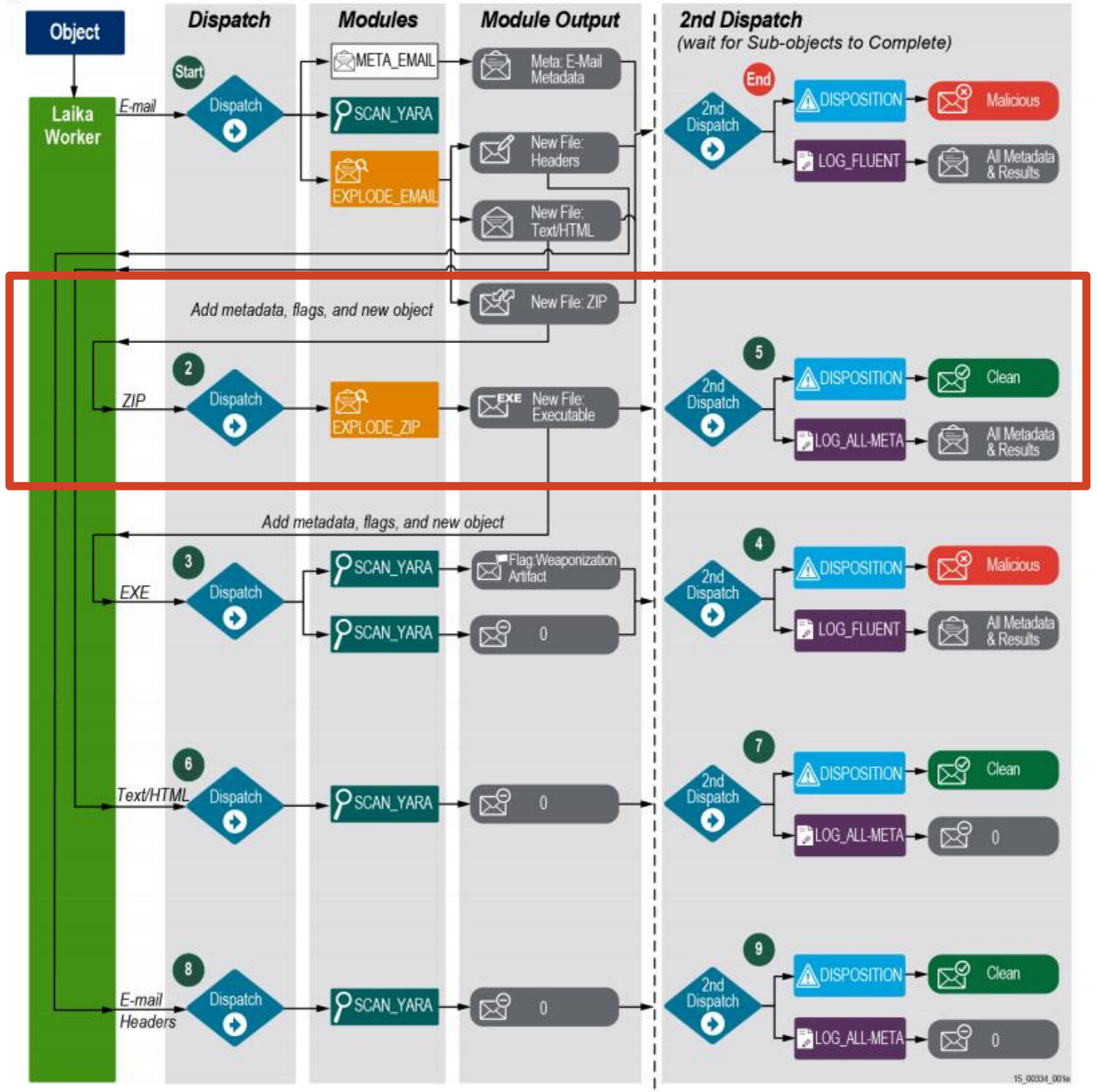
Laika BOSS

READING AN EMAIL



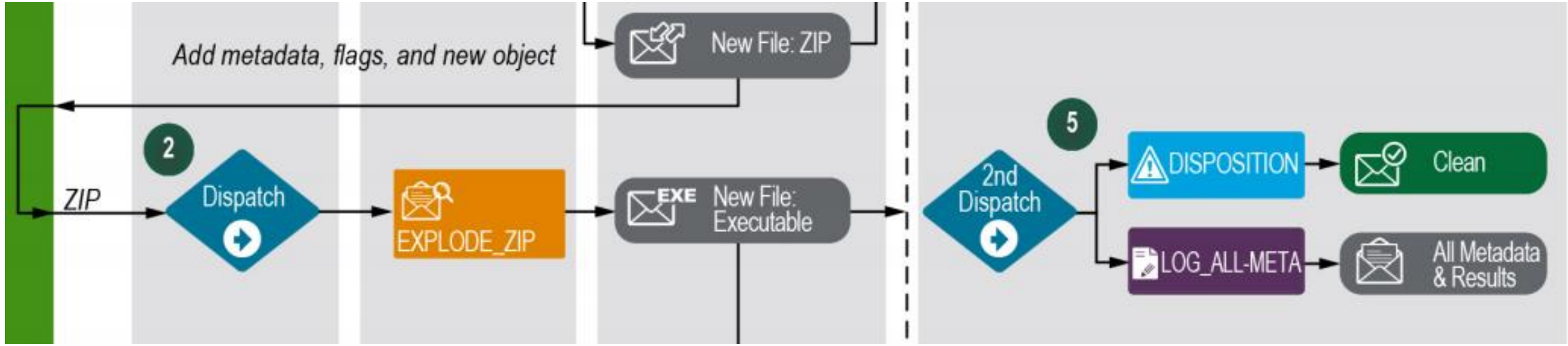
Laika BOSS

READING AN EMAIL



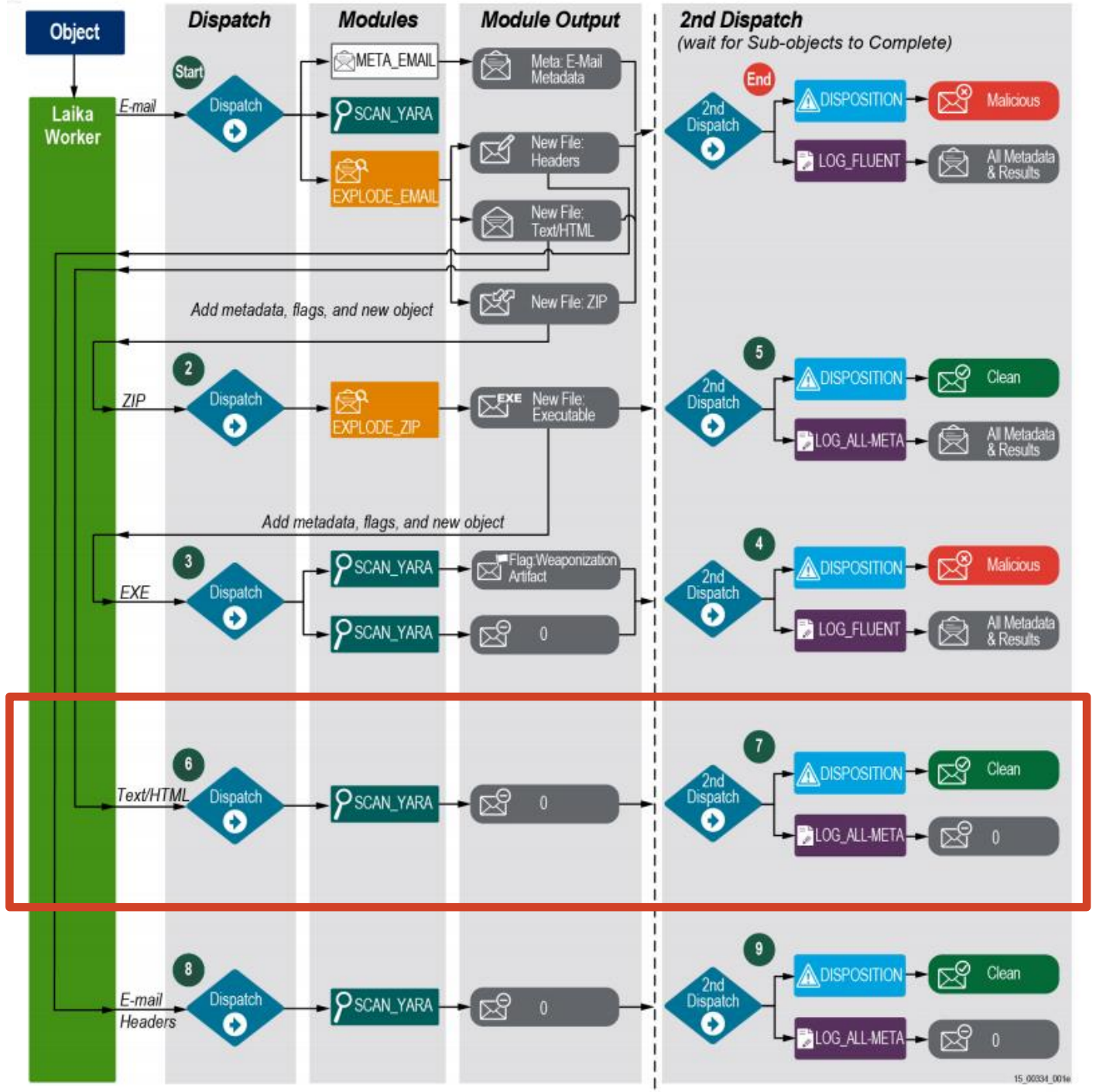
Laika BOSS

READING AN EMAIL



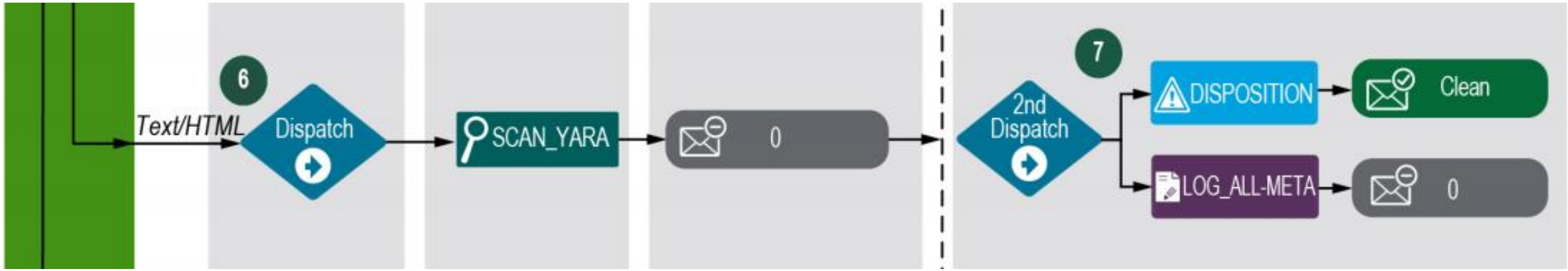
Laika BOSS

READING AN EMAIL



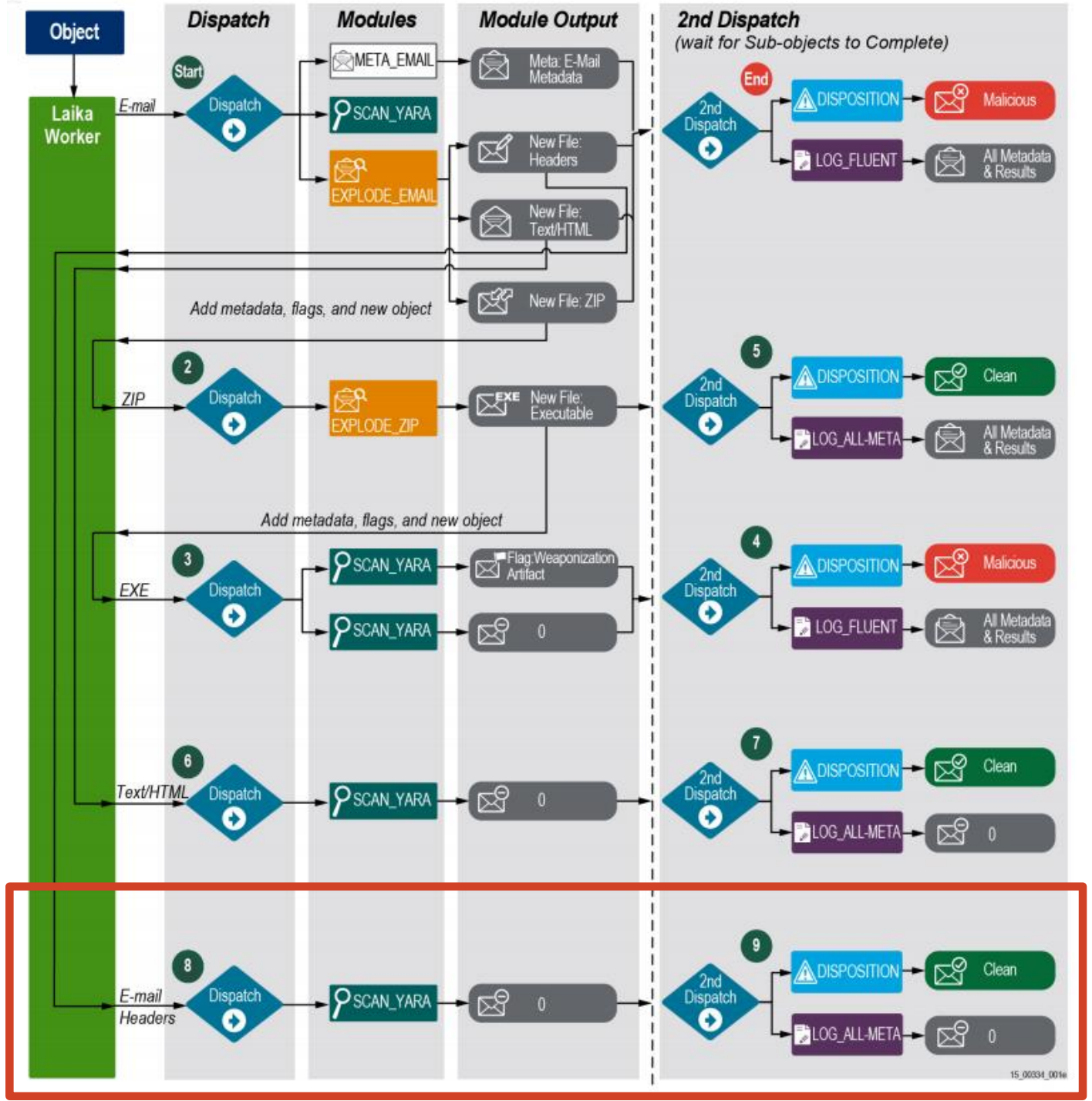
Laika BOSS

READING AN EMAIL



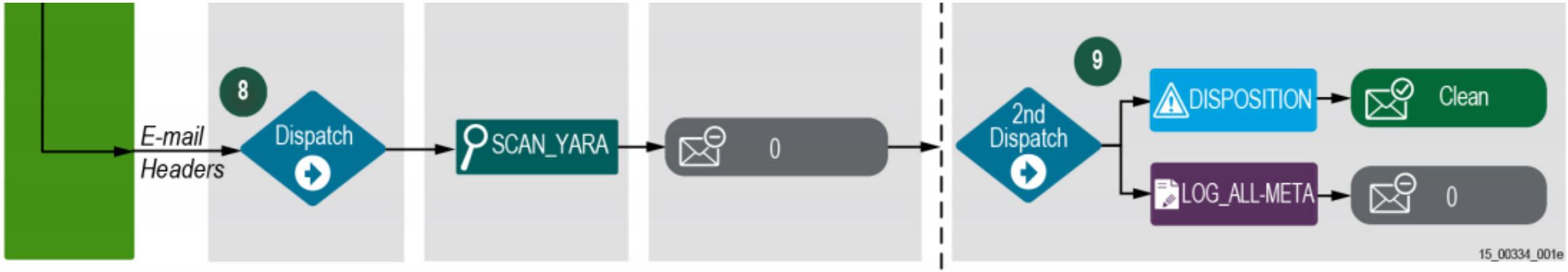
Laika BOSS

READING AN EMAIL



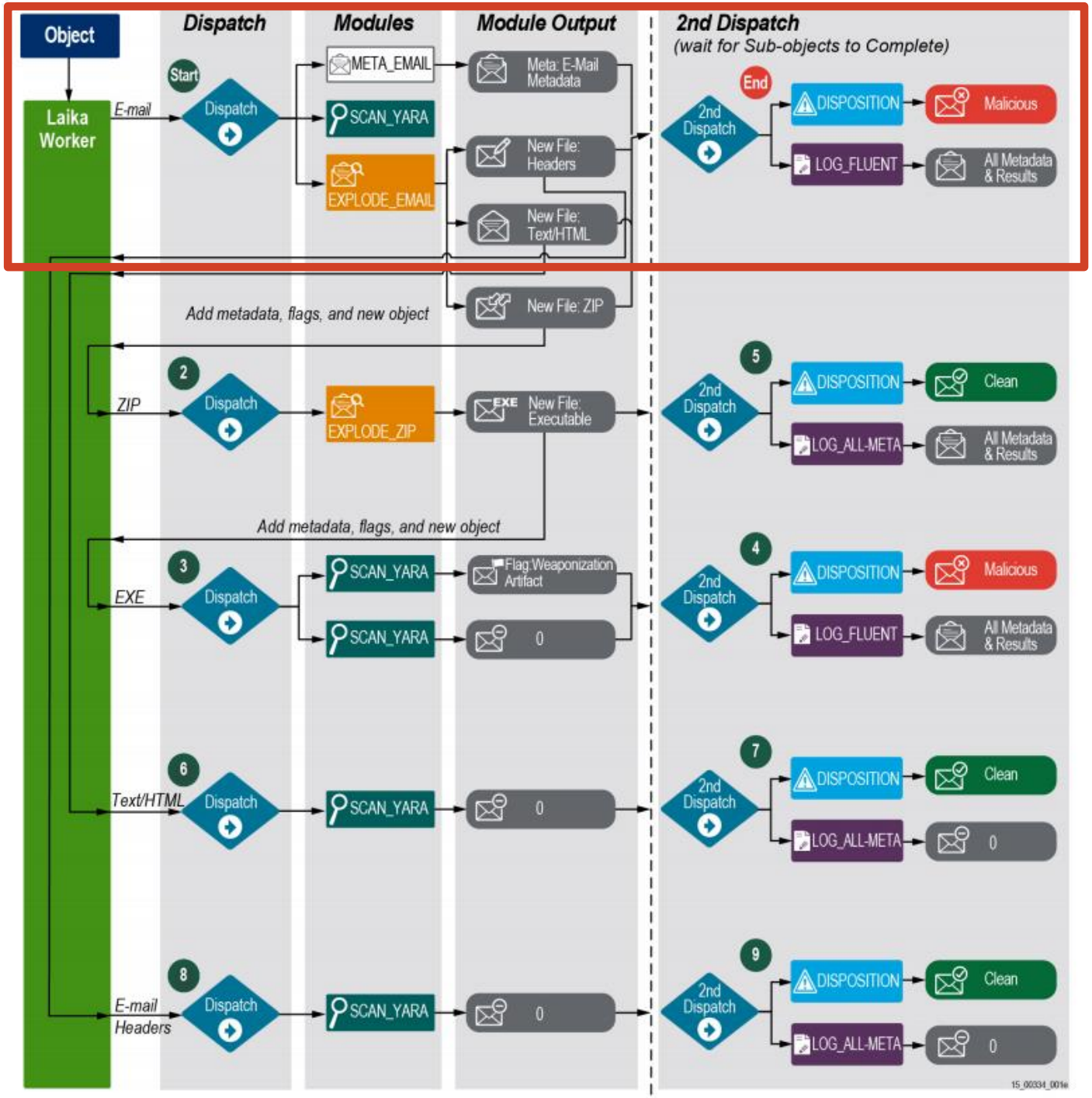
Laika BOSS

READING AN EMAIL



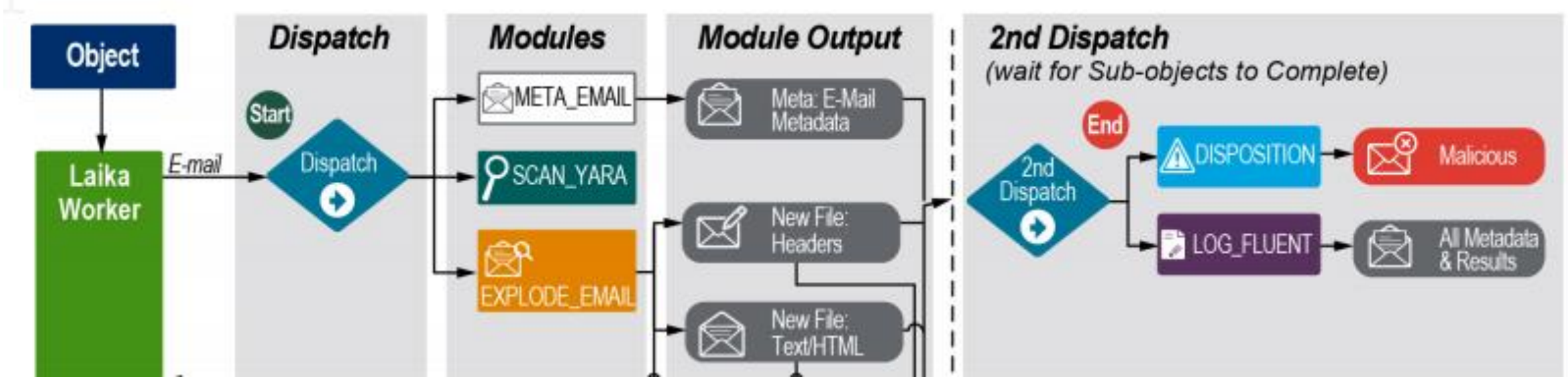
Laika BOSS

READING AN EMAIL



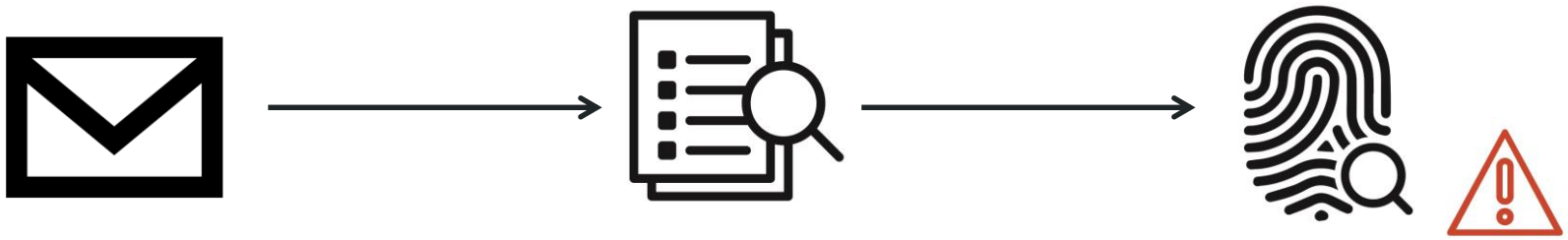
Laika BOSS

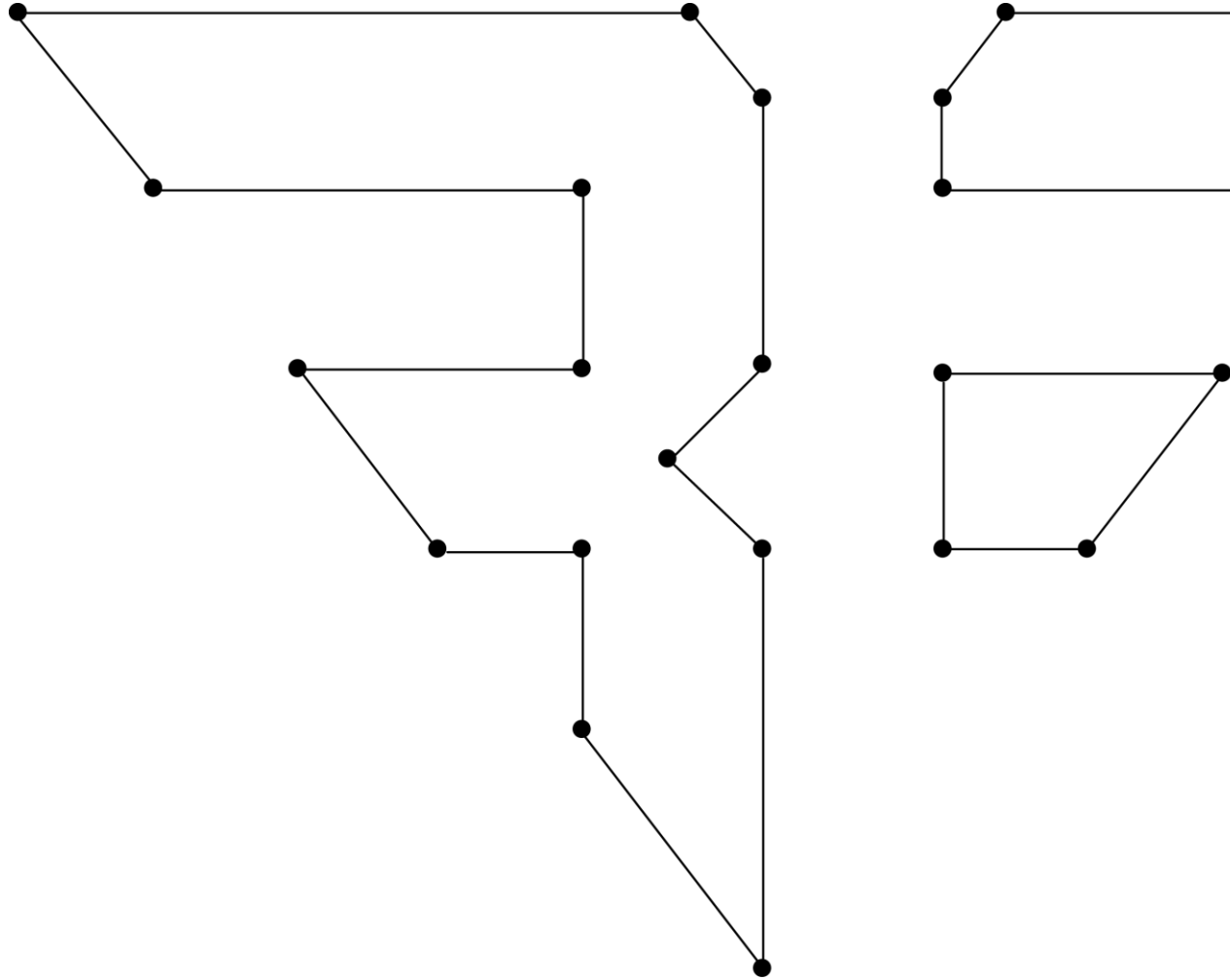
READING AN EMAIL



Simplified View

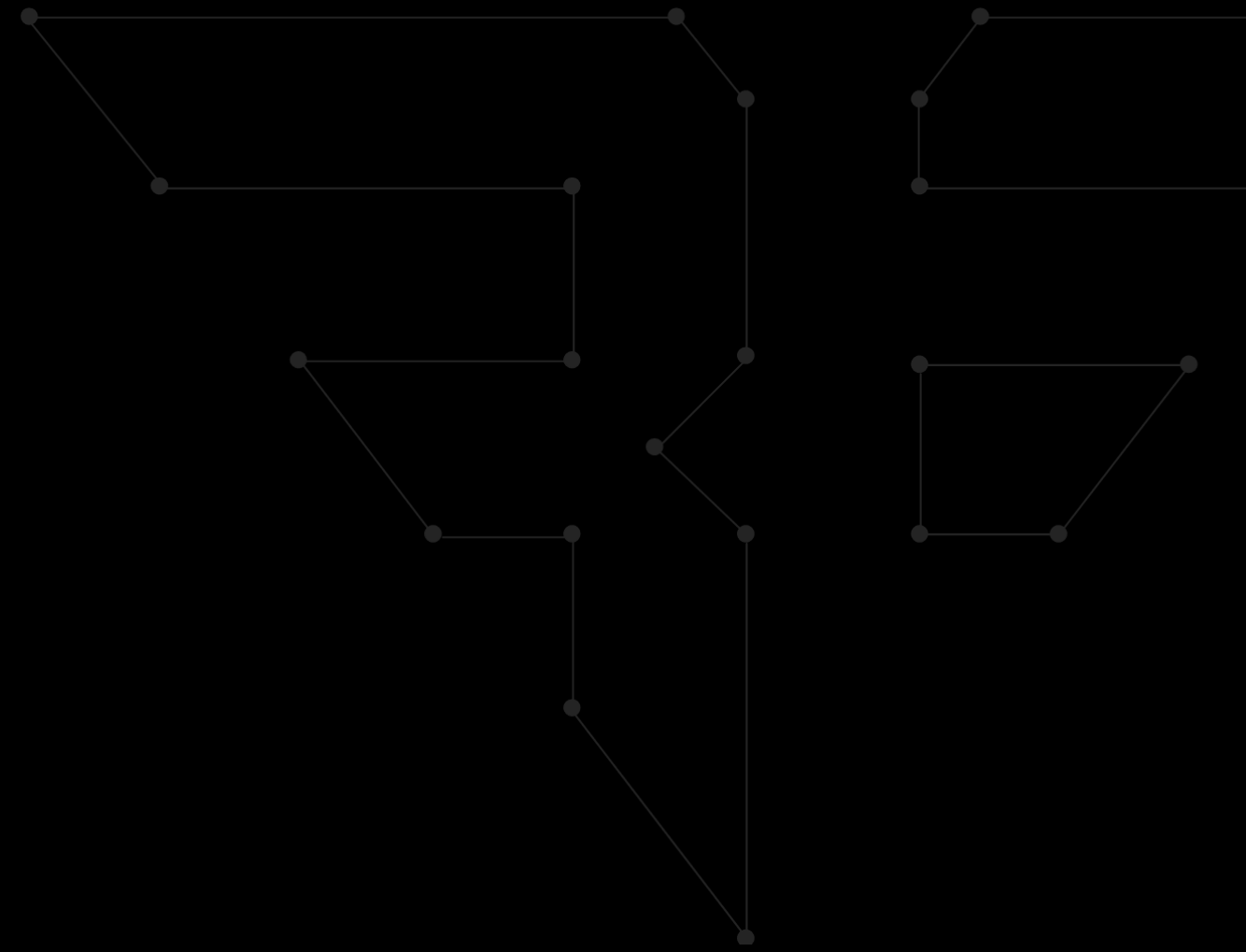
MAYBE A LITTLE OVER SIMPLIFIED





DEMONSTRATION

WHAT COULD GO WRONG?



USE CASES

IS IT USEFUL?

Use Cases

HOW CAN I USE LAIKA BOSS?

- Interfaces with Milter (Mail Filter) to reject malicious emails
- File metadata capture for CIRT
  - What employees are downloading
  - What customers are uploading
- Integration with a web content filter to filter out files from being downloaded

PRODUCT CONSIDERATIONS

WHAT TO WATCH OUT FOR

Considerations

WHAT ARE THE FAILURES?

Type Recognition

- Laika BOSS only recognizes 32 types out of the box.

Support

- Built by Lockheed Martin, no commercial support.

Setting it up

- The product is flexible, but setting it up isn’t just the push of a button.

Type Recognition

OUT-OF-THE-BOX

Types known out of the box

jar	hlp
pem	wri
der	lnk
crt	class
pkcs7	eml
pe	mime
zip	tnef
rar	fws
cab	cws
tar	zws
arj	swf
ole	tiff
officex	mp3
rtf	wmv
pdf	avi
chm	mov

VirusShare_00220.zip (9.8GB)

```
56326 0.85948 empty
7471 0.11400 pe
474 0.00723 rar
404 0.00616 zip
143 0.00218 jar
16 0.00024 cab
8 0.00012 ole
7 0.00011 swf
6 0.00009 cws
1 0.00002 mime
1 0.00002 officex
1 0.00002 pdf
1 0.00002 zws
```

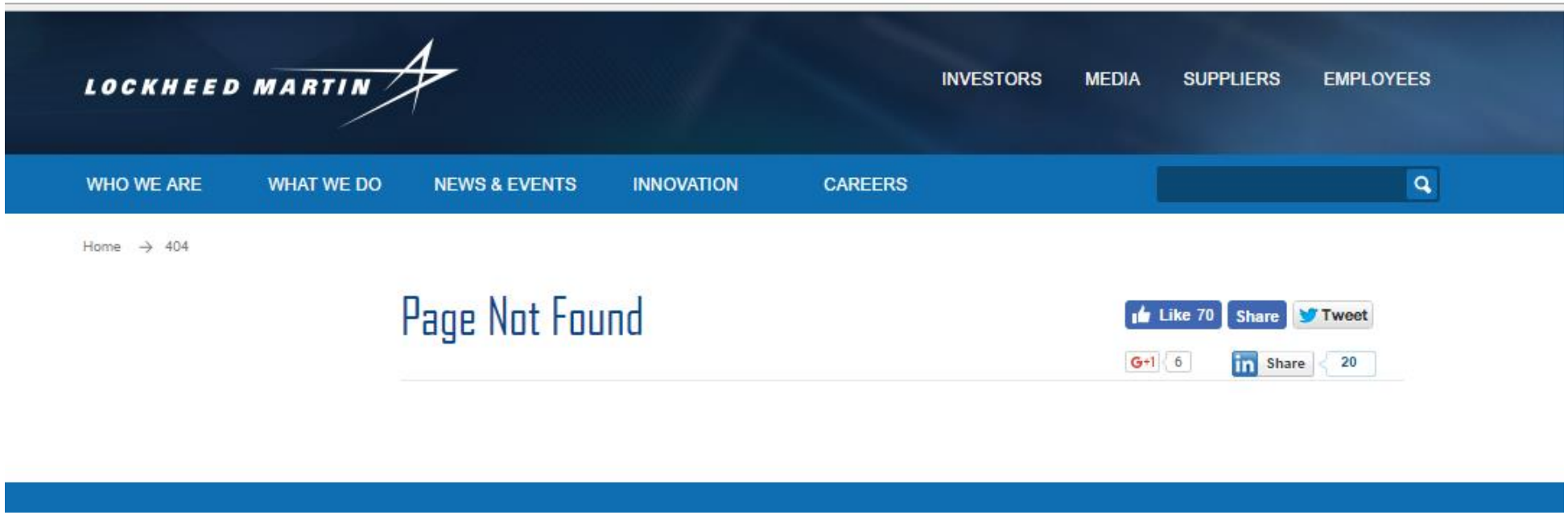
Support

OR LACK THEREOF

LAIKA BOSS · Lockheed Martin

www.lockheedmartin.com/us/what-we.../information.../laika-boss.ht... ▾ Lockheed Martin ▾

Laika BOSS is a **file**-centric malware analysis tool and intrusion detection system provided as an open-source offering. Developed by Lockheed Martin, **Laika** ...



Setting it up

HOW TO TRY TO USE IT

Out-of-the-box

- OOB, the product does relatively little

Setup and customization is a must

- In order to get much out of the product, customization is required.

```
$ ./laika.py ~/test_files/testfile.cws.swf | jq
'.scan_result[] | { "file type" : .fileType, "flags" :
.flags, "md5" : .objectHash }'
100%[##############################################]
Processed: 1/1 total files (Elapsed Time: 0:00:00)
Time: 0:00:00
{
  "md5": "dffcc2464911077d8ecd352f3d611ecc",
  "flags": [],
  "file type": [
    "cws",
    "swf"
  ]
}
{
  "md5": "587c8ac651011bc23ecefecd4c253cd4",
  "flags": [],
  "file type": [
    "fws",
    "swf"
  ]
}
```

Thank You

BISHOP FOX®