



Kestrel

<https://github.com/opencybersecurityalliance/kestrel-lang>

An Open Source Cyber Threat Hunting Language implemented in Python with multiple collaboration opportunities:

Threat Hunting Systemization

- Huntbook Authoring
- Hunting Library Development

Integration And Automation

- Data Source Adaptors
- Execute Kestrel Via OpenC2/CACAO
- Automated hunting

Kestrel Customization And Extension

- Analytics, AI/ML, And Threat Intelligence
- Use Cases And Solutions
- Language Extensions
- Visualizations

Quick Glance at the Kestrel Way

Huntbooks (Jupyter Notebooks) used for the Black Hat USA 2022 Demo

1. standard way to search TTPs
2. connect the dots without ETL
3. bring your existing code/binary
4. automate with OpenC2

Ps at any complexity could be described as graph patterns, pointed

NodeJS

A process

binary: not NodeJS

a process spawns a process invoking another binary/image

le 1 on Windows: reading email results in executing someth

```
g_candidates = GET process
FROM stixshifter://bh22-windows-192.168.56.
WHERE [process:parent_ref.name = 'WinMail.e
START t'2022-07-01T00:00:00Z' STOP t'2022-08
```

ishing_candidates ATTR pid, name, command_line

le 2 on Linux: a web service is exploited to spawns a mali

```
_candidates = GET process
FROM stixshifter://bh22-linux-192.168.56.91
WHERE [process:parent_ref.name = 'node' AND
START t'2022-07-01T00:00:00Z' STOP t'2022-08
```

exploit_candidates ATTR pid, name, command_line

name
cmd.exe
cmd.exe C:\Windows\system32\cmd.exe /c ""C:\Users\Alice\AppData\Local\Temp
xplore.exe
xplore.exe "C:\Program Files\Internet Explorer
name

```
# process 7880 on 192.168.56.111 looks like an exploit
# similar cross-host data-flow tracking via network tra

lateral_mov_linux = splunkd_activities WHERE pid = 7880
lateral_mov_linux_nt = FIND network-traffic CREATED BY
DISP lateral_mov_linux_nt ATTR src_ref.value, src_port,
```

src_ref.value	src_port	dst_ref.value	dst_port
192.168.56.111	50383	192.168.56.91	80

Block Executed in 1 seconds

VARIABLE	TYPE	# (ENTITIES)	# (RECORDS)	directory*	file
lateral_mov_linux	process	3	4	0	
lateral_mov_linux_nt	network-traffic	1	1	146	14

*Number of related records cached.

```
lateral_mov_91_nt = GET network-traffic FROM stixshifter
WHERE [network-traffic:src_port = 1

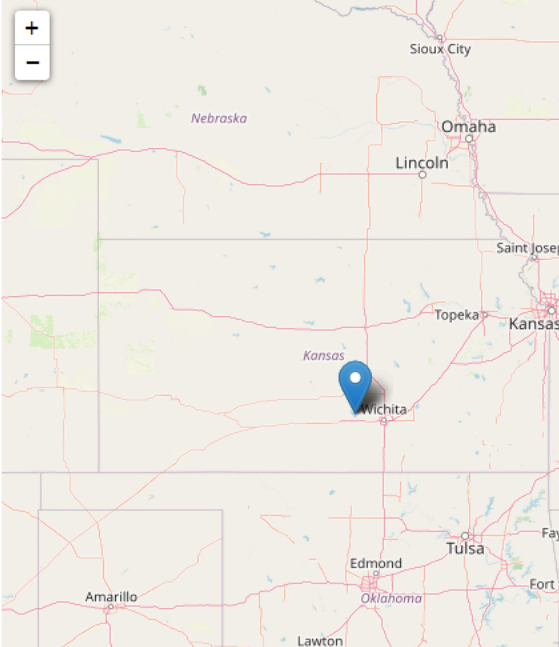
DISP lateral_mov_91_nt ATTR src_ref.value, src_port, ds

linux_proc = FIND process CREATED lateral_mov_91_nt
DISP linux_proc ATTR pid, name, command_line
```

src_ref.value	src_port	dst_ref.value	dst_port
192.168.56.111	50383	172.17.0.2	80

172.17.0.2	38508	104.86.237.27	443	a104-86-237-27.depl
172.17.0.2	38522	104.17.123.99	443	
172.17.0.2	38524	140.82.113.4	443	
172.17.0.2	38538	65.8.66.113	443	server-

```
# https://github.com/opencybersecurityalliance/kestrel-
APPLY python://pin-IP-on-map ON traffic
```



```
cmd = {
  "action": "investigate",
  "target": {
    "process": {
      "name": "node"
    }
  },
  "args": {
    "huntargs": {},
    "returnvars": ["exploits"],
    "response_requested": "complete"
  },
  "actuator": {
    "x-kestrel": {
      "huntbook": "exploits"
    }
  }
}

response = run_command(cmd)
pd.DataFrame(response['results']['exploits'])
```

response from server: 200

	binary_ref.id	binary_ref.name	binary_ref.parent_directory_ref.i
0	file-449b2085-5f61-5d58-bfd9-399e1fa4684d	node	directory--e7436cdd-f067-5c1e-9fd9-ad0ff5cd38
1	file-449b2085-5f61-5d58-bfd9-399e1fa4684d	node	directory--e7436cdd-f067-5c1e-9fd9-ad0ff5cd38
2	file-34603467-34c1-50ee-bc09-	sh	directory--1e950b10-638e-5c9e-8363-897b04d8c5f

Kestrel Portal

<https://github.com/opencybersecurityalliance/kestrel-lang>
pcoccoli@us.ibm.com xiaokui.shu@ibm.com

star the kestrel repo


opencybersecurityalliance / kestrel-langPublic

NotificationsFork 41Star 204

<> CodeIssues 47Pull requests 2ActionsProjectsSecurityInsights

develop3 branches43 tagsGo to fileCode

README.rst



Kestrel

pythoncode styleblackcodecov 83%pypi v1.5.9downloads 552/monthdocs passing

[News] Kestrel hunt at Infosec Jupyterthon 2022 [J'22 live hunt recording]

[News] Kestrel session at Black Hat USA 2022 [BH'22 recording | BH'22 hunting lab]

Kestrel is a threat hunting language aiming to make cyber threat hunting fast by providing a layer of abstraction to build reusable, composable, and shareable hunt-flow.

Try Kestrel in a cloud sandbox without install (Blog: Try Kestrel in a Cloud Sandbox).

Software developers write Python or Swift than machine code to quickly turn business logic into applications. Threat hunters write Kestrel to quickly turn threat hypotheses into hunt-flow. We see threat hunting as an interactive procedure to create customized intrusion detection systems on the fly, and hunt-flow is to hunts as control-flow is to ordinary programs.

What does it mean by hunt fast?

- Do not write the same TTP pattern in different data source queries.
- Do not write one-time-use adapters to connect hunt steps.

About

Kestrel threat hunting language: building reusable, composable, and shareable huntflows across different data sources and threat intel.

language security threat cybersecurity threat-hunting threatintel hacktoberfest security-automation security-tools threat-intelligence

ReadmeApache-2.0 license204 stars14 watching41 forks

Releases 43v1.5.9 Latest last week + 42 releases

Contributors 11

Documentation

Huntbooks

Kestrel

Installation And Setup / Install Runtime

What is Kestrel?

Installation And Setup

General Requirements

OS-specific Requirements

Choose Where to Install

opencybersecurityalliance / kestrel-huntbookPublic

NotificationsFork 4Star 21

<> CodeIssues 2Pull requests 0Discussions 0Actions 0Projects 0Wiki 0Security 0Insights

main2 branches0 tagsGo to fileCode

subbyte update 1st huntbook in tutorial267966 last week83 commits

blackhat22 update Black Hat USA 22 huntbooks for Kestrel v1.54 months ago

config clean up stixshifter config7 months ago

huntbooks fix datasource in Lateral Movement6 months ago

tutorial update 1st huntbook in tutoriallast week

CHANGELOG.rst refresh binder service with kestrel-lang 1.5.4last month

LICENSE.md Create LICENSE.md2 years ago

README.md typo fix7 months ago

About

This repository hosts community contributed Kestrel huntflows (.hf) and huntbooks (.pynb)

ReadmeView license21 stars10 watching4 forks

Releases

No releases published

Packages

No packages published

Contributors 4

subbyte Xiaokui Shu

pcoccoli Paul Coccoli

OASIS-OP-Admin

JasonKirstead Jason Kirstead

Jupyter

FilesRunningClusters

Select items to perform actions on them.

demo

images

templates

1. Start Hunt From TTPs.pynb

Name

Last Modified

File size

seconds ago

a month ago

a month ago

a month ago

a month ago

a month ago

a month ago

a month ago

706 kB

OPEN CYBERSECURITY ALLIANCE

Fun with securitydatasets.com and the Kestrel PowerShell Deobfuscator

Published by Paul Coccoli on October 31, 2022

threat hypothesis A variant A.2

threat hypothesis A

Latest Articles

Introducing the Indicators of Behavior (IOB) Sub-Project

Open Cybersecurity Alliance Adds Indicators of Behavior (IoB) Sub-Project

Fun with securitydatasets.com and

Hunting Labs

Technical Blogs

© 2024 IBM Corporation

3