Detecting macOS Compromise with Venator

SPECTER OPS

HELLO!

I am Richie Cyrus

Defensive Services Team @ SpecterOps

Former Detection & Response @Apple

SPECTER OPS

The number of macOS systems in the enterprise is growing.

SPECTER OPS

macOS malware is alive and trending upward.

Defensive controls will eventually fail or be bypassed.

cybereason

SentinelOne™

Carbon Black.

CROWDSTRIKE

cybere on
SentinelOne™
Carb n Blac
CROWDSTRIKE

VirusTotal
{JSON}
JavaScript Object Notation
SPECTER OPS

INTRODUCING

VENATOR

A macOS tool for proactive detection of malicious activity.

SPECTER OPS

Launch Agents

Launch Daemons

Browser Extensions

Event Taps

Applications

Bash History

Gatekeeper Status

Network Connections

SIP Status

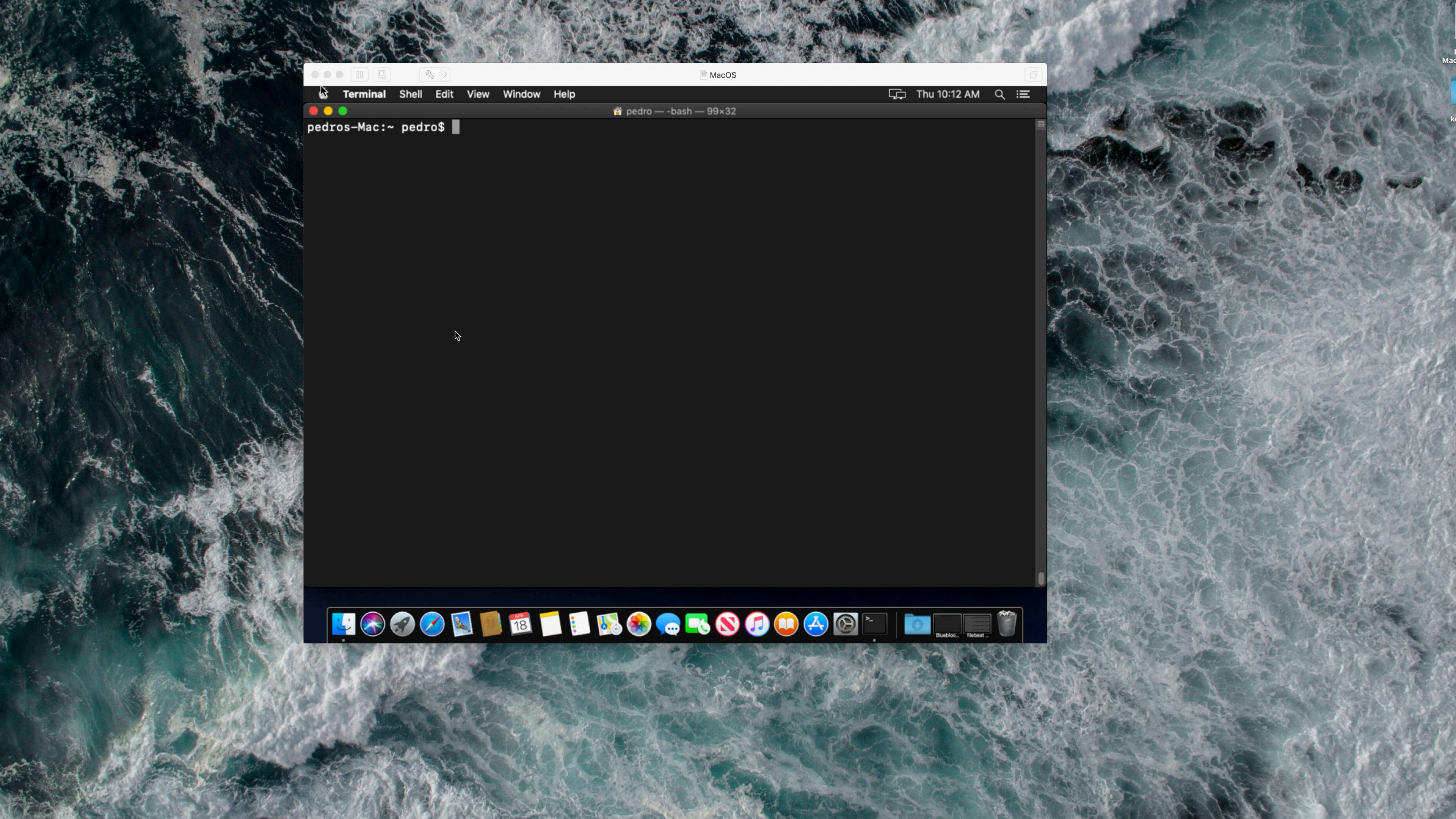
Login Items

Cron Jobs

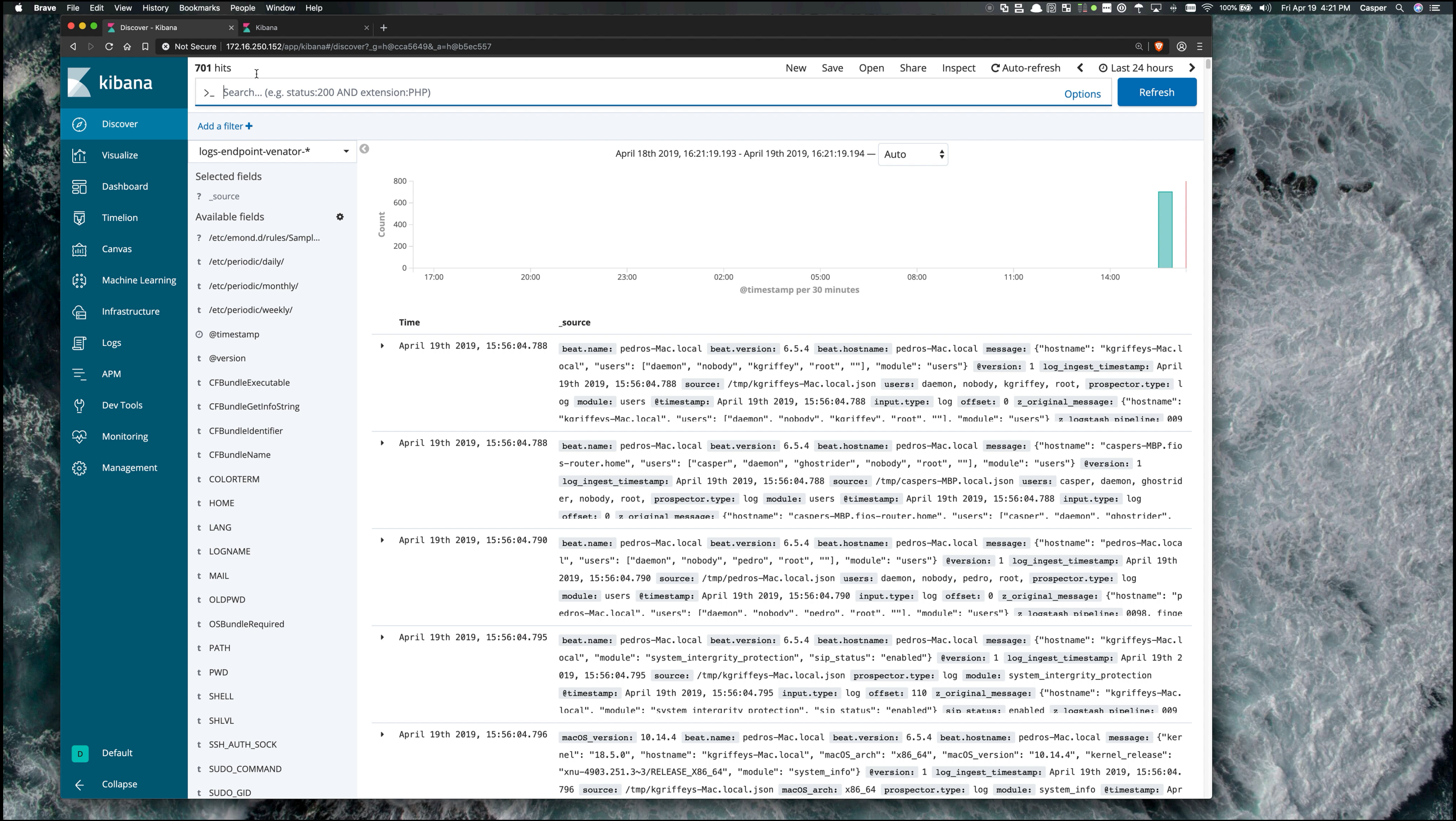
Env Variables

System Info

richieRich-MacBook-Pro.json



```
pedros-Mac:~ pedro$ 
```



```
April 19th 2019, 15:56:04.788   beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "kgriffeys-Mac.l
                                ocal", "users": ["daemon", "nobody", "kgriffey", "root", ""], "module": "users"} @version: 1 log_ingest_timestamp: April
                                19th 2019, 15:56:04.788 source: /tmp/kgriffeys-Mac.local.json users: daemon, nobody, kgriffey, root, prospector.type: l
                                og module: users @timestamp: April 19th 2019, 15:56:04.788 input.type: log offset: 0 z_original_message: {"hostname":
                                "kgriffeys-Mac.local", "users": ["daemon", "nobody", "kgriffey", "root", ""], "module": "users"} z_logstash_pipeline: 009

April 19th 2019, 15:56:04.788   beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "caspers-MBP.fio
                                s-router.home", "users": ["casper", "daemon", "ghostrider", "nobody", "root", ""], "module": "users"} @version: 1
                                log_ingest_timestamp: April 19th 2019, 15:56:04.788 source: /tmp/caspers-MBP.local.json users: casper, daemon, ghostrid
                                er, nobody, root, prospector.type: log module: users @timestamp: April 19th 2019, 15:56:04.788 input.type: log
                                offset: 0 z_original_message: {"hostname": "caspers-MBP.fios-router.home", "users": ["casper", "daemon", "ghostrider",

April 19th 2019, 15:56:04.790   beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "pedros-Mac.loca
                                l", "users": ["daemon", "nobody", "pedro", "root", ""], "module": "users"} @version: 1 log_ingest_timestamp: April 19th
                                2019, 15:56:04.790 source: /tmp/pedros-Mac.local.json users: daemon, nobody, pedro, root, prospector.type: log
                                module: users @timestamp: April 19th 2019, 15:56:04.790 input.type: log offset: 0 z_original_message: {"hostname": "p
                                edros-Mac.local", "users": ["daemon", "nobody", "pedro", "root", ""], "module": "users"} z_logstash_pipeline: 0098, finge

April 19th 2019, 15:56:04.795   beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "kgriffeys-Mac.l
                                ocal", "module": "system_intergrity_protection", "sip_status": "enabled"} @version: 1 log_ingest_timestamp: April 19th 2
                                019, 15:56:04.795 source: /tmp/kgriffeys-Mac.local.json prospector.type: log module: system_intergrity_protection
                                @timestamp: April 19th 2019, 15:56:04.795 input.type: log offset: 110 z_original_message: {"hostname": "kgriffeys-Mac.
                                local", "module": "system_intergrity_protection", "sip_status": "enabled"} sip_status: enabled z_logstash_pipeline: 009

April 19th 2019, 15:56:04.796   macOS_version: 10.14.4 beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"ker
                                nel": "18.5.0", "hostname": "kgriffeys-Mac.local", "macOS_arch": "x86_64", "macOS_version": "10.14.4", "kernel_release":
                                "xnu-4903.251.3~3/RELEASE_X86_64", "module": "system_info"} @version: 1 log_ingest_timestamp: April 19th 2019, 15:56:04.
                                796 source: /tmp/kgriffeys-Mac.local.json macOS_arch: x86_64 prospector.type: log module: system_info @timestamp: Apr
```

Future Updates

External Log Shipping

Support for sending output .JSON files to external location (ie. Amazon S3 bucket)

Additional Modules

Downloaded files, .bashrc, File in /tmp, and more!

Any questions?

You can find me on Twitter:

@rrcyrus

@SpecterOps

SPECTER OPS