

Detecting macOS Compromise with Venator

HELLO!

I am Richie Cyrus

Defensive Services Team @ SpecterOps

Former Detection & Response @Apple

The number of macOS systems in the enterprise is growing.

macOS malware is alive and trending upward.

***Defensive controls will eventually fail or
be bypassed.***



Carbon Black.





cyberark
ΣΥΡΕΛΛΗΞΗ



SentinelOne™

Carbon Black



CROWDSTRIKE





VirusTotal

{JSON}

JavaScript Object Notation

JavaScript Object Notation



SPECTER OPS

INTRODUCING VENATOR

A macOS tool for
proactive detection of
malicious activity.



Launch Agents

Launch Daemons

Browser Extensions

Event Taps

Applications

Bash History

Gatekeeper Status

Network Connections

SIP Status

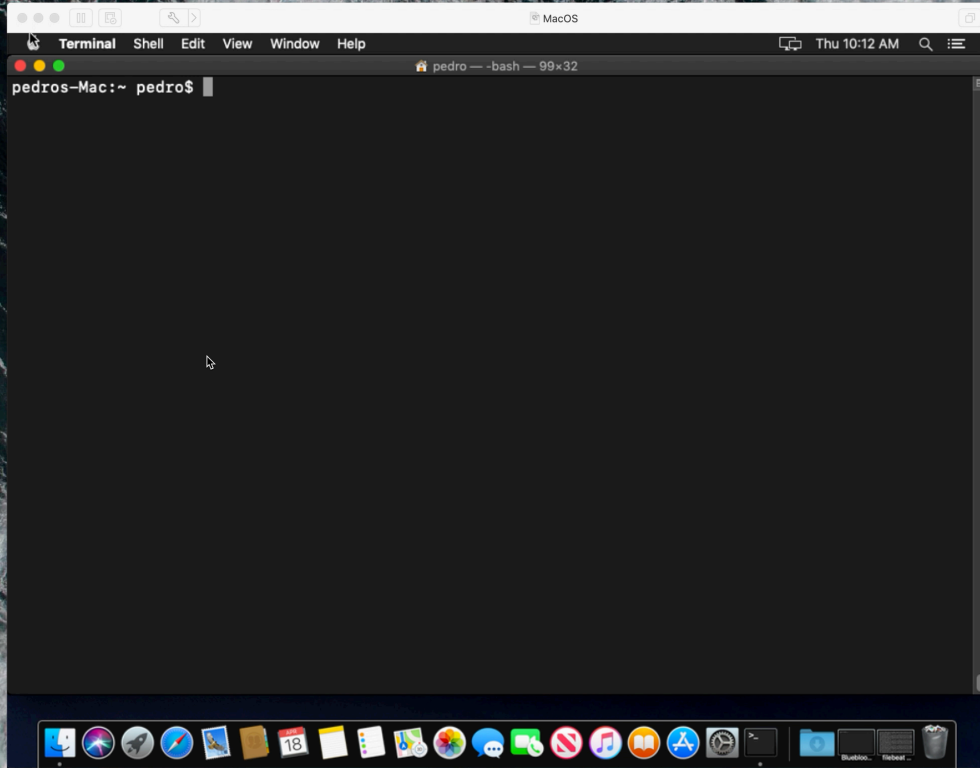
Login Items

Cron Jobs

Env Variables

System Info

richieRich-MacBook-Pro.json





701 hits

New Save Open Share Inspect Auto-refresh Last 24 hours

> Search... (e.g. status:200 AND extension:PHP)

Options

Refresh

Add a filter +

logs-endpoint-venator-*

April 18th 2019, 16:21:19.193 - April 19th 2019, 16:21:19.194 Auto

Selected fields

? _source

Available fields

? /etc/emond.d/rules/Sampl...

t /etc/periodic/daily/

t /etc/periodic/monthly/

t /etc/periodic/weekly/

o @timestamp

t @version

t CFBundleExecutable

t CFBundleGetInfoString

t CFBundleIdentifier

t CFBundleName

t COLORTERM

t HOME

t LANG

t LOGNAME

t MAIL

t OLDPWD

t OSBundleRequired

t PATH

t PWD

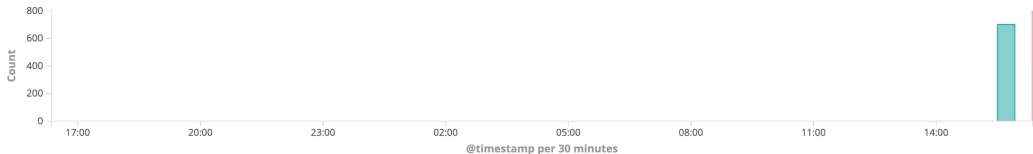
t SHELL

t SHLVL

t SSH_AUTH_SOCK

t SUDO_COMMAND

t SUDO_GID



Time	_source
▶ April 19th 2019, 15:56:04.788	<code>beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "kgriffeys-Mac.local", "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: log module: users @timestamp: April 19th 2019, 15:56:04.788 input.type: log offset: 0 z_original_message: {"hostname": "kgriffeys-Mac.local". "users": ["daemon". "nobadv". "koriffey". "root". ""]. "module": "users"} z_loastash pipeline: 009</code>
▶ April 19th 2019, 15:56:04.788	<code>beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "caspers-MBP.fios-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, ghostrider, 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". "nhostrider".</code>
▶ April 19th 2019, 15:56:04.790	<code>beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "pedros-Mac.local", "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": "pedros-Mac.local". "users": ["daemon". "nobadv". "nedro". "root". ""]. "module": "users"} z_loastash pipeline: 0098. finne</code>
▶ April 19th 2019, 15:56:04.795	<code>beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"hostname": "kgriffeys-Mac.local", "module": "system_integrity_protection", "sip_status": "enabled"} @version: 1 log_ingest_timestamp: April 19th 2019, 15:56:04.795 source: /tmp/kgriffeys-Mac.local.json prospector.type: log module: system_integrity_protection @timestamp: April 19th 2019, 15:56:04.795 input.type: log offset: 110 z_original_message: {"hostname": "Kgriffeys-Mac.local". "module": "system interarivty protection". "sip status": "enabled"} sip status: enabled z_loastash pipeline: 009</code>
▶ April 19th 2019, 15:56:04.796	<code>macOS_version: 10.14.4 beat.name: pedros-Mac.local beat.version: 6.5.4 beat.hostname: pedros-Mac.local message: {"kernel": "18.5.0", "hostname": "Kgriffeys-Mac.local", "macOS_arch": "x86_64", "macOS_version": "10.14.4", "kernel_release": "xnu-4903.251.3-3/RELEASE_ARM_T8040", "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</code>

Default

Collapse

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