VMware Carbon Black® Cloud Managed Detection™ Monthly Report

August 2019

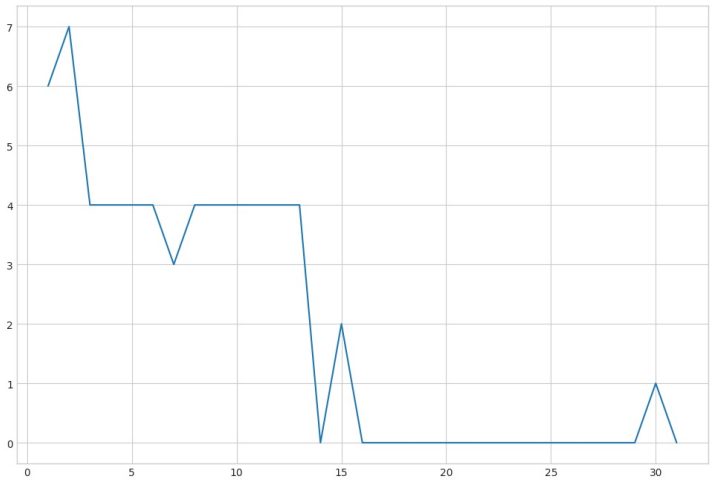
01. Most Common Suspicious Events

The most frequent alerts detected during this reporting period, along with the number of different devices that each was detected on.

Description	Count	# Devices
A known virus (PUP: Mimikatz) was detected running.	52	1
A PUP or Potentially Unwanted Program (PUP: Mimikatz) was detected.	2	1
A known virus (Trojan: Mimikatz) was detected.	2	1
A known virus (Downloader: Swabfex) was detected.	1	1
A known virus (Downloader: Donoff) was detected.	1	1
A known virus (PUP: Mimikatz) was detected running. A Deny Policy Action was applied	1	1

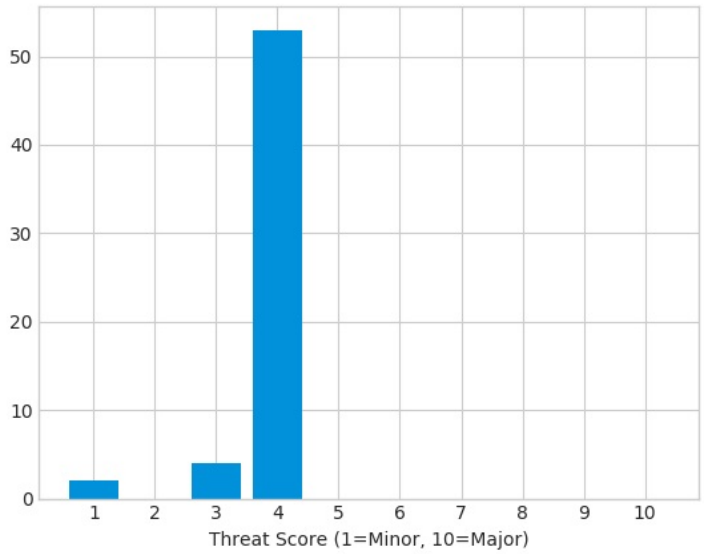
02. Daily Alerts

An overview of the total number of alerts detected per day across all devices.



03. Threat Score Breakdown

A breakdown of the most commonly occurring threat scores for monitored events and threats last month.



04. Top Targeted Endpoints

The devices with the most alerts during the reporting period, along with the number of distinct files (by hash) that caused an alert on each.

Device ID	Alerts Issued	Distinct Files
20571	52	1
21212	5	3
17126	2	2

05. Top Suspect Applications by Name

The applications (by name) that generated the most alerts last month, along with the number of different devices each was detected on.

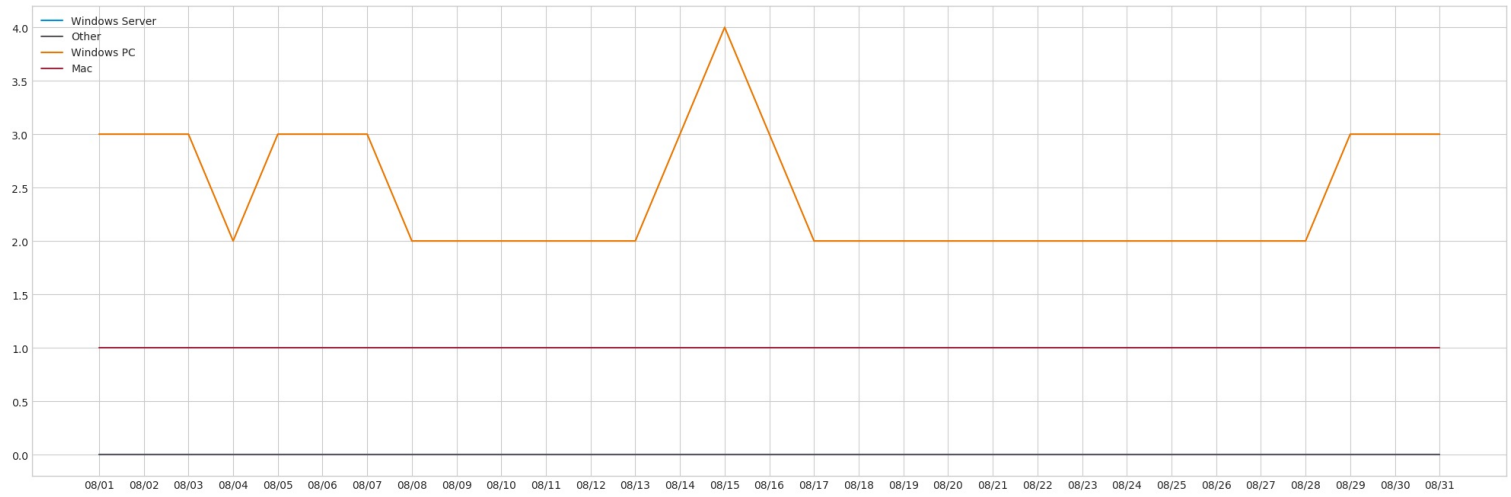
Description	Occurrences	Distinct Devices
mimikatz.exe	52	1
RepMgr.exe	6	2
cmd.exe	1	1

VMware Carbon Black® Cloud Managed Detection™ Monthly Report

August 2019

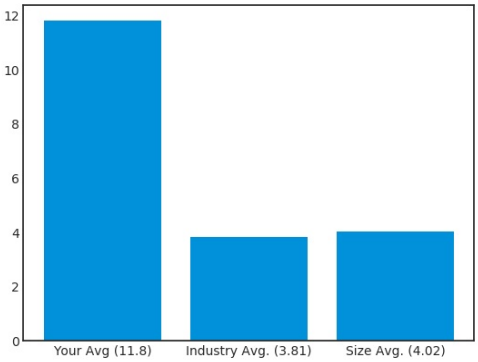
06. Active Sensors by Type

The number of sensors that reported events to our servers each day, by operating system type.



07. Market Segment Comparison

A comparison of the average number of threats per device in your organization vs. others in your industry (government) and organization size (medium).



08. Most Common OS Versions

The most common operating system versions detected in your environment.

OS Version	# of Devices
Windows 8 x64	1
Windows 10 x86	1
MAC OS X 10.12.0	1
Windows 10 x64	1
Windows 7 x64 SP: 1	1

09. Top Targeted Users

The non-administrative users that were involved in the most alerts last month, along with the number of distinct files (by hash) that caused alerts.

Name	Alerts Issued	Distinct Files
1	22	1
2	1	1
3	22	1
4	22	1
5	22	1
6	22	1
7	22	1
8	22	1
9	22	1
10	22	1

10. Most Widespread User Names

These user names were associated with alerts on the most distinct devices, which may or may not indicate unauthorized access.

Description	Distinct Devices
1	1
2	1

VMware Carbon Black® Cloud Managed Detection™ Monthly Report

August 2019

11. New Alerts This Month

These specific alerts were detected this month, but not in the previous month. These may represent novel attacks or otherwise noteworthy new behavior on your devices.

Description	Distinct Devices
A PUP or Potentially Unwanted Program (PUP: Mimikatz) was detected.	1
A known virus (Downloader: Swabfex) was detected.	1
A known virus (Downloader: Donoff) was detected.	1
A known virus (PUP: Mimikatz) was detected running.12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890	1
A known virus (PUP: Mimikatz) was detected running. A Deny Policy Action was applied	1
A known virus (Trojan: Mimikatz) was detected.	1

12. New Suspicious Applications This Month

These specific application names had alerts during the last month, but not in the previous month. These may represent novel attacks or otherwise interesting new behavior on your devices.

App Name	Alert	Distinct Devices
RepMgr.exe	A known virus (Trojan: Mimikatz) was detected.	2
mimikatz.exe	A known virus (PUP: Mimikatz) was detected running.	1
cmd.exe	A known virus (PUP: Mimikatz) was detected running. A Deny Policy Action was applied.12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890	1