McAfee MVISION Mobile

SIEM Integration Guide

September 2018

Contents

Introduction

Organizational security solutions provide a wealth of forensic security information. Disparate systems funnel this information into a centralized security repository that IT Security departments use to dissect security events coming in from across your enterprise. This information is then used to combat the external and internal security threats your organization sees on a day to day basis.

This centralized security information repository is referred to as a Security Information and Event Management (SIEM) system. It provides a real-time view into the alerts generated by network hardware (Firewalls, IDS/IPS, Web Filters, Email Filters, etc) and applications across your enterprise, and with the use of McAfee's solution, your end user mobile devices as well.

Implementation

When a security event is generated from one of your devices, the event information including relevant forensics are uploaded into your McAfee MVISION Mobile Console. This data can be pulled down to your environment and placed in a directory that your SIEM system polls for data import. The data is presented in JSON format, which provides an easy way for any SIEM to be able to digest the event and associated forensics.

To pull these events down to your environment so that they can be imported in to your SIEM server, McAfee Support needs to perform a one-time configuration and provide you with security parameters required. At some point this configuration is available in the McAfee MVISION Mobile Console user interface.

These security events can now be retrieved by the customer using HTTPS and a secure access token:

1) Make a connection to the McAfee MVISION Mobile Console Authentication server to provide security information and retrieve an access security token.
2) Use this security token when requesting logs from the McAfee MVISION Mobile Console. Only logs not yet retrieved are returned.
3) Store the logs in a directory that the SIEM has access to.
4) The SIEM periodically scans this directory for new logs and imports the data contained in them.
5) Repeat every X minutes to ensure new events coming in are imported as well.

Syslog Pull Module

McAfee has provided a sample script (Appendix A) to retrieve security events. It is a starting point and can be modified by your company as needed. The Syslog Pull Module (SPM) is a bash script which runs CURL commands to access your McAfee MVISION Mobile Console securely. The output of the CURL command (which are your security events in JSON format) is stored directly into a file.

This folder for the written files is monitored by a standard SIEM such as Splunk forwarder (this is decided by the customer's system). This makes sure that the contents of the file are imported by the SIEM.

The SPM should be run in crontab to pull events. It is important to note the following:

- The SPM automatically generates a new file for each request to the McAfee server.
- The SPM cleans up old files (configured currently to clean up files older than a week).
- Requests are made over HTTPS.

Hardware/Software Requirements

- It is preferable that the system run on a Linux machine. The SPM is a bash script but can be converted by the customer to whatever language is needed.
- CURL is required to be installed on the machine.
- The SPM bash script must have permissions to call CURL.
- CURL must have permissions to write a file to the destination folder.
- In this example, a Splunk Monitor must be configured to monitor the destination.
- At least 5GB free space on the hard drive.

Event Selection

Event records are coded with the Severity Type according to the selection in the Threat Response Policy:

Severity Type	Code
Normal	0
Low	1
Elevated	2
Critical	3

By default all Severity Types are returned in the response to the Sylog Pull. If it is required to only see certain severity types, that can be controlled by using the 'severity' parameter in the request URL. Only events for the severity type matching the code above are returned. If more than one severity type is required, reference the 'severity' parameter for each code.

Forensic Data Elements

McAfee provides two options for the number of forensic elements that are contained within each syslog event. The syslog feature can be configured return all forensics (Verbose) or just the event metadata (Concise) depending on the amount of log information required by teams consuming the information. Verbose mode provides the most extensive log information currently available. To select which mode is used in your collection, the request URL can be modified to select either mode, Verbose is the default if the 'level' parameter is not supplied:

SYSLOG Samples

The sample script in Appendix A details how to request events to be imported. The following sections detail the fields in syslog output for each mode:

Note: Every field in the table below shows whether the field is "available" for all threat types or some threat types. The following describes the availability:

- **All Threats** - This field is available for All Threat Types
- **Multiple Threats** - This field is available for more than 1 Threat Type
- **Specific Threat** - This field is available for only 1 Threat Type

Concise Mode

Name	Description
device_info Availability: All Threats	Device Information
device_info.app Availability: All Threats	App name reporting the Threat Events
device_info.app_version Availability: All Threats	App version reporting the Threat Events
device_info.device_time Availability: All Threats	Timestamp on the device at the time of event
device_info.imei Availability: All Threats	Unique Device ID
device_info.jailbroken Availability: All Threats	Jailbroken Status
device_info.model Availability: All Threats	Device Model
device_info.operator Availability: All Threats	Mobile Network Operator

device_info.os Availability: All Threats	Operating System
device_info.os_version Availability: All Threats	Operating System Version
device_info.tag1 Availability: All Threats	Unique Tag from SDK
device_info.tag2 Availability: All Threats	Unique Tag from SDK
device_info.type Availability: All Threats	Device Name/Model
event_id Availability: All Threats	Threat Event Identifier
eventtimestamp Availability: All Threats	Timestamp at the time of event
location Availability: All Threats	User Device location
location.accuracy Availability: All Threats	Accuracy
location.country_name Availability: All Threats	Country Name
location.exact Availability: All Threats	Is this a GPS Location ?
location.p Availability: All Threats	Current User Device GPS location
location.p.[n] Availability: All Threats	Current User Device GPS location
location.previous_sample Availability: All Threats	Previous User Device GPS location
location.previous_sample.p Availability: All Threats	Previous User Device GPS location
location.previous_sample.p.[n]	Previous User Device GPS location

Availability: All Threats	
location.previous_sample.time Availability: All Threats	Previous Location Sampling Timestamp
location.previous_sample.time.$date Availability: All Threats	Previous Location Sampling Timestamp
location.sampled_time Availability: All Threats	Location Sampling Timestamp
location.sampled_time.$date Availability: All Threats	Location Sampling Timestamp
location.source Availability: All Threats	GPS or Geo IP Address
location.state_name Availability: All Threats	State
mitigated Availability: All Threats	End user action taken
severity Availability: All Threats	Threat Severity
threat Availability: All Threats	Threat Information
threat.general Availability: All Threats	Threat General Information
threat.general.action_triggered Availability: All Threats	Action Triggered on the User Device
threat.general.attacker_bssid Availability: Multiple Threats	Attacker MAC Address of the Wireless Access Point
threat.general.attacker_ip Availability: Multiple Threats	Attacker Device IP Address
threat.general.attacker_mac Availability: Multiple Threats	Attacker Device MAC Address
threat.general.attacker_ssid Availability: Multiple Threats	Attacker Network Name of the Wireless Access Point

threat.general.basestation Availability: All Threats	Cellular Basestation Information
threat.general.basestation.mnc Availability: All Threats	Mobile Network Code
threat.general.basestation.psc Availability: All Threats	Primary Scrambling Code
threat.general.basestation.type Availability: All Threats	Basestation Type
threat.general.basestation.cid Availability: All Threats	Cell ID
threat.general.basestation.mcc Availability: All Threats	Mobile Country Code
threat.general.basestation.lac Availability: All Threats	Location Area Code
threat.general.certificate Availability: Multiple Threats	SSL Certificate collected
threat.general.change_type Availability: Multiple Threats	Change Type
threat.general.device_ip Availability: All Threats	User Device IP
threat.general.device_mac Availability: All Threats	User Device MAC Address
threat.general.device_time Availability: All Threats	User Device Timestamp
threat.general.dns_after_change Availability: Threat Specific	DNS IP After Change
threat.general.dns_before_change Availability: Threat Specific	DNS IP Before Change
threat.general.event Availability: Threat Specific	Reason for the detection
threat.general.external_ip	User Device External IP Address

Availability: All Threats	
threat.general.file_hash Availability: Threat Specific	File Hash of the Download or Installed App
threat.general.file_name Availability: Threat Specific	File Path of the Downloaded or Installed App
threat.general.file_path Availability: Threat Specific	File Path of the File System changed
threat.general.gateway_after_change Availability: Threat Specific	Gateway IP After Change
threat.general.gateway_before_change Availability: Threat Specific	Gateway IP Before Change
threat.general.gateway_ip Availability: All Threats	User Device Gateway IP
threat.general.gateway_mac Availability: All Threats	User Device Gateway MAC Address
threat.general.imei Availability: All Threats	Unique Device ID
threat.general.jailbreak_reasons Availability: Multiple Threats	Reasons for the Jailbreak detection
threat.general.malware_list Availability: All Threats	Malware Threat Family Name, Score
threat.general.network Availability: All Threats	Network Name where the User Device was connected at the time of event
threat.general.network_bssid Availability: All Threats	Network BSSID where the User Device was connected at the time of event
threat.general.process Availability: Multiple Threats	Process Name
threat.general.proxy_after_change Availability: Threat Specific	Proxy IP After Change
threat.general.sideloaded_app_developer Availability: Multiple Threats	Developer of the Sideloaded App

threat.general.sideloaded_app_name Availability: Threat Specific	App Name of the Sideloaded App
threat.general.sideloaded_app_package Availability: Threat Specific	Package Name of the Sideloaded App
threat.general.stagefright_vulnerability_report Availability: Threat Specific	Stagefright CVE List
threat.general.suspected_url Availability: Multiple Threats	Suspicious URL
threat.general.suspicious_profile_info Availability: Multiple Threats	Suspicious Profile Information
threat.general.suspicious_profile_name Availability: Multiple Threats	Suspicious Profile Name
threat.general.suspicious_profile_type Availability: Multiple Threats	Suspicious Profile Type
threat.general.threat_type Availability: All Threats	Threat Name
threat.general.time_interval Availability: All Threats	Time that passed since connecting to the network (in seconds)
threat.name Availability: All Threats	Threat Name
threat.story Availability: All Threats	Threat Summary
user_info Availability: All Threats	User Information
user_info.employee_name Availability: All Threats	End User Name on McAfee MVISION Mobile Console
user_info.user_email Availability: All Threats	End User Email on McAfee MVISION Mobile Console
user_info.user_group Availability: All Threats	End User Group on McAfee MVISION Mobile Console
user_info.user_role	End User Role on McAfee MVISION Mobile

Availability: All Threats	Console

Verbose Mode

Items in Verbose mode are added to the items already collected in Concise mode.

Name	Description
forensics Availability: All Threats	Forensics Information
forensics.BSSID Availability: All Threats	MAC Address of the Wireless Access Point (BSSID)
forensics.SSID Availability: All Threats	Network Name
forensics._id Availability: All Threats	McAfee Internal Field
forensics._id.$oid Availability: All Threats	McAfee Internal Field
forensics.android_compatibility_check_response Availability: Multiple Threats	Android Compatibility Check Response collected for the threats "Android Device Compatibility Not Test By Google" and "Android Device Possible Tampering"
forensics.app_tampering_reasons Availability: Threat Specific	Reasons to detect App Tampering Event
forensics.attack_time Availability: All Threats	Unix Timestamp at the time of event
forensics.attack_time.$date Availability: All Threats	Unix Timestamp at the time of event
forensics.baseline_traceroute Availability: Threat Specific	McAfee Internal Field
forensics.captive_portal_after Availability: Multiple Threats	HTML Response collected for the McAfee URL after the attack

forensics.captive_portal_before Availability: Multiple Threats	HTML Response collected for the McAfee URL before the attack
forensics.close_networks Availability: All Threats	Android shows the Nearby Networks and iOS shows the current connected Network
forensics.close_networks.[n] Availability: All Threats	Android shows the Nearby Networks and iOS shows the current connected Network
forensics.close_networks.[n].BSSID Availability: All Threats	Android shows the BSSID of the Nearby Networks and iOS shows the BSSID of the current connected Network
forensics.close_networks.[n].SSID Availability: All Threats	Android shows the Network Name (SSID) of the Nearby Networks and iOS shows the Network Name (SSID) of the current connected Network
forensics.close_networks.[n].capabilities Availability: All Threats	Wireless Security Protocols supported by the Nearby Networks e.g. WEP, WPA, WPA2
forensics.close_networks.[n].frequency Availability: All Threats	Frequency of the Nearby Networks e.g. 2.4 Ghz, 5 Ghz
forensics.close_networks.[n].level Availability: All Threats	Signal Strength (-35 to -95)
forensics.dangerzone_nearby_wifi Availability: Multiple Threats	Suspicious Nearby Network
forensics.directory_entries Availability: All Threats	Files listed in the /usr/lib/ folder of an iOS device
forensics.directory_entries.[n] Availability: All Threats	Files listed in the /usr/lib/ folder of an iOS device
forensics.directory_entries.[n].file_name Availability: All Threats	File Name of the files in the /usr/lib/ folder of an iOS device
forensics.directory_entries.[n].file_size Availability: All Threats	File Size of the files in the /usr/lib/ folder of an iOS device
forensics.directory_entries.[n].hash Availability: All Threats	File Hash of the files in the /usr/lib/ folder of an iOS device

forensics.directory_entries.[n].is_symlink Availability: All Threats	Files listed is a symlink or not in the /usr/lib/ folder of an iOS device
forensics.directory_entries.[n].nlink Availability: All Threats	Number of hard links of the files listed in the /usr/lib/ folder of an iOS device
forensics.directory_entries.[n].permission Availability: All Threats	Permission of the files listed in the /usr/lib/ folder of an iOS device
forensics.file_system_change Availability: Threat Specific	File System Change event
forensics.file_system_change.change_type Availability: Threat Specific	Type of File System Change
forensics.file_system_change.event Availability: Threat Specific	Reason for the File System Change
forensics.file_system_change.full_path Availability: Threat Specific	Path of the File System Change
forensics.general Availability: All Threats	General Information of the Event
forensics.general.[n] Availability: All Threats	General Information of the Event
forensics.general.[n].name Availability: All Threats	Multiple fields
forensics.general.[n].type Availability: All Threats	Multiple fields
forensics.general.[n].val Availability: All Threats	Multiple fields
forensics.host_attack Availability: All Threats	Device Attack - Event Information
forensics.host_attack.application Availability: Threat Specific	App Name of the Suspicious Android App
forensics.host_attack.daemon_minflt Availability: Threat Specific	McAfee Internal Field

forensics.host_attack.daemon_minflt.[n] Availability: Threat Specific	McAfee Internal Field
forensics.host_attack.daemon_rss Availability: Threat Specific	McAfee Internal Field
forensics.host_attack.daemon_rss.[n] Availability: Threat Specific	McAfee Internal Field
forensics.host_attack.detected_locally Availability: Threat Specific	Detection source: zDB or Cogito
forensics.host_attack.file_hash Availability: Threat Specific	Hash of the File Download or Installed
forensics.host_attack.filename Availability: Threat Specific	Name of the File Download or Installed
forensics.host_attack.info_after Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.info_after.selinux_context Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.info_after.user_id Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.info_before Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.info_before.selinux_context Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.info_before.user_id Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.is_blacklisted Availability: Threat Specific	If the iOS App is Blacklisted by the Admin
forensics.host_attack.is_malicious Availability: Threat Specific	If the iOS App is already listed as Malicious in the database
forensics.host_attack.malware_detection_source Availability: Multiple Threats	Detection Source 0 means Local and 1 means Remote

forensics.host_attack.malware_matches Availability: Multiple Threats	Malware Information
forensics.host_attack.malware_matches.[n] Availability: Multiple Threats	Malware Information
forensics.host_attack.malware_matches.[n].name Availability: Multiple Threats	Malware Threat Family Name
forensics.host_attack.malware_matches.[n].score Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.malware_matches.[n].signatures Availability: Threat Specific	McAfee Internal Field
forensics.host_attack.malware_matches.[n].signatures.[n] Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.malware_matches.[n].signatures.[n].hash Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.malware_matches.[n].signatures.[n].size Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.malware_matches.[n].signatures.[n].type Availability: Multiple Threats	McAfee Internal Field
forensics.host_attack.malware_scan_category Availability: Multiple Threats	0 means App downloaded and 1 means App Installed
forensics.host_attack.malware_threat_name Availability: Threat Specific	Malware Threat Family Name
forensics.host_attack.process Availability: Multiple Threats	Process Name
forensics.host_attack.process_pid Availability: Multiple Threats	Process ID
forensics.host_attack.suspected_url Availability: Multiple Threats	Suspicious URL

forensics.json_jailbreak_reasons Availability: Multiple Threats	Reasons for the Jailbreak detection
forensics.mitm_traceroute Availability: Threat Specific	McAfee Internal Field
forensics.network_threat Availability: All Threats	Network Forensics
forensics.network_threat.arp_tables Availability: All Threats	ARP Tables
forensics.network_threat.arp_tables.after Availability: All Threats	ARP Tables collected seconds after detecting the attack
forensics.network_threat.arp_tables.after.table Availability: All Threats	ARP Tables collected seconds after detecting the attack
forensics.network_threat.arp_tables.after.table.[n] Availability: All Threats	ARP Tables collected seconds after detecting the attack
forensics.network_threat.arp_tables.after.table.[n].ip Availability: All Threats	IP Address in the ARP Tables collected seconds after detecting the attack
forensics.network_threat.arp_tables.after.table.[n].mac Availability: All Threats	MAC Address in the ARP Tables collected seconds after detecting the attack
forensics.network_threat.arp_tables.before Availability: All Threats	ARP Tables collected seconds before detecting the attack
forensics.network_threat.arp_tables.before.table Availability: All Threats	ARP Tables collected seconds before detecting the attack
forensics.network_threat.arp_tables.before.table.[n] Availability: All Threats	ARP Tables collected seconds before detecting the attack
forensics.network_threat.arp_tables.before.table.[n].ip Availability: All Threats	IP Address in the ARP Tables collected seconds before detecting the attack
forensics.network_threat.arp_tables.before.table.[n].mac Availability: All Threats	MAC Address in the ARP Tables collected seconds before detecting the attack
forensics.network_threat.arp_tables.initial Availability: All Threats	ARP Tables collected when the device was initially to the network

forensics.network_threat.arp_tables.initial.table Availability: All Threats	ARP Tables collected when the device was initially to the network
forensics.network_threat.arp_tables.initial.table.[n] Availability: All Threats	ARP Tables collected when the device was initially to the network
forensics.network_threat.arp_tables.initial.table.[n].ip Availability: All Threats	IP Address in the ARP Tables collected when the device was initially to the network
forensics.network_threat.arp_tables.initial.table.[n].mac Availability: All Threats	MAC Address in the ARP Tables collected when the device was initially to the network
forensics.network_threat.attacker_ip Availability: All Threats	IP Address of the Attacker's Device
forensics.network_threat.attacker_mac Availability: Multiple Threats	MAC Address of the Attacker's Device
forensics.network_threat.basestation Availability: All Threats	Cellular Basestation Information
forensics.network_threat.basestation Availability: All Threats	Mobile Network Code
forensics.network_threat.basestation Availability: All Threats	Primary Scrambling Code
forensics.network_threat.basestation Availability: All Threats	Basestation Type
forensics.network_threat.basestation Availability: All Threats	Cell ID
threat.general.basestation.mcc Availability: All Threats	Mobile Country Code
threat.general.basestation.lac Availability: All Threats	Location Area Code
forensics.network_threat.delta_route_cache Availability: Multiple Threats	McAfee Internal Field
forensics.network_threat.delta_route_cache.table Availability: Multiple Threats	McAfee Internal Field

forensics.network_threat.delta_route_cache.table.[n] Availability: All Threats	McAfee Internal Field
forensics.network_threat.delta_route_cache.table.[n].gateway Availability: All Threats	McAfee Internal Field
forensics.network_threat.delta_route_cache.table.[n].ip Availability: All Threats	McAfee Internal Field
forensics.network_threat.gw_ip Availability: All Threats	User Gateway IP Address
forensics.network_threat.gw_mac Availability: All Threats	User Gateway MAC Address
forensics.network_threat.interface Availability: All Threats	User Device Network Interface
forensics.network_threat.my_ip Availability: All Threats	User Device IP Address
forensics.network_threat.my_mac Availability: All Threats	User Device MAC
forensics.network_threat.net_stat Availability: All Threats	Device Network Status Information
forensics.network_threat.net_stat.[n] Availability: All Threats	Device Network Status Information
forensics.network_threat.net_stat.[n].Foreign Address Availability: All Threats	Foreign Host and Port with connection state
forensics.network_threat.net_stat.[n].Local Address Availability: All Threats	Local Host and Port with connection state
forensics.network_threat.net_stat.[n].Proto Availability: All Threats	Protocol
forensics.network_threat.net_stat.[n].Recv-Q Availability: All Threats	Represents data in queue for the socket waiting to read

forensics.network_threat.net_stat.[n].Send-Q Availability: All Threats	Represents data in queue for the socket waiting to be sent
forensics.network_threat.net_stat.[n].State Availability: All Threats	Socket State
forensics.network_threat.routing_table Availability: All Threats	Routing Table Information
forensics.network_threat.routing_table.[n] Availability: All Threats	Routing Table Information
forensics.network_threat.routing_table.[n].Destination Availability: All Threats	Destination Network IP
forensics.network_threat.routing_table.[n].Flags Availability: All Threats	-
forensics.network_threat.routing_table.[n].Gateway Availability: All Threats	Network Gateway IP
forensics.network_threat.routing_table.[n].Netif Availability: All Threats	Network Interface e.g. lo (local interface), wlan0 (wireless interface), rmnet (cellular network)
forensics.network_threat.routing_table.[n].Refs Availability: All Threats	-
forensics.network_threat.routing_table.[n].Use Availability: All Threats	-
forensics.os Availability: All Threats	Operating System
forensics.probabilities Availability: All Threats	McAfee Internal Field
forensics.probabilities.[n] Availability: All Threats	McAfee Internal Field
forensics.process_list Availability: All Threats	Device Process List
forensics.process_list.[n] Availability: All Threats	Device Process List collected at the time of the event

forensics.process_list.[n].Parent process(PPID) Availability: All Threats	Parent Process ID
forensics.process_list.[n].Process ID(PID) Availability: All Threats	Process ID
forensics.process_list.[n].Process Name Availability: All Threats	Process Name
forensics.process_list.[n].Service Availability: All Threats	Process Service
forensics.process_list.[n].User Availability: All Threats	Process Username
forensics.proxy_conf Availability: Multiple Threats	Proxy Configuration
forensics.proxy_conf.ip_after Availability: Multiple Threats	Proxy Configuration: IP Address After change
forensics.proxy_conf.ip_before Availability: Multiple Threats	Proxy Configuration: IP Address Before change
forensics.responses Availability: All Threats	Device Action Triggered
forensics.responses.[n] Availability: All Threats	Device Action Triggered
forensics.rogue_access_point Availability: Multiple Threats	Rogue Access Point information
forensics.rogue_access_point.BSSID Availability: Multiple Threats	MAC Address of the Wireless Access Point
forensics.rogue_access_point.SSID Availability: Multiple Threats	Network Name
forensics.rogue_access_point.frequency Availability: Multiple Threats	Frequency
forensics.routing_table Availability: All Threats	Routing Table Information

forensics.routing_table.[n] Availability: All Threats	Routing Table Information
forensics.routing_table.[n].destination Availability: All Threats	Destination Network IP
forensics.routing_table.[n].flags Availability: All Threats	-
forensics.routing_table.[n].gateway Availability: All Threats	Network Gateway IP
forensics.routing_table.[n].netif Availability: All Threats	-
forensics.routing_table.[n].refs Availability: All Threats	-
forensics.routing_table.[n].use Availability: All Threats	-
forensics.sample_data Availability: All Threats	McAfee Internal Field
forensics.severity Availability: All Threats	Threat Severity
forensics.sideloaded_app_developer Availability: Multiple Threats	Developer of the Sideloaded App
forensics.sideloaded_app_name Availability: Threat Specific	App Name of the Sideloaded App
forensics.sideloaded_app_package Availability: Threat Specific	Package Name of the Sideloaded App
forensics.ssl_downgrade_description Availability: Multiple Threats	McAfee Internal Field
forensics.ssl_mitm_certificate Availability: Multiple Threats	SSL Certificate collected
forensics.ssl_strip_reply Availability: Multiple Threats	HTML Response collected

forensics.stagefright_vulnerability_report Availability: Threat Specific	Stagefright CVE List
forensics.suspicious_profile Availability: Multiple Threats	Suspicious Profile Information
forensics.suspicious_profile.profile_information Availability: Multiple Threats	Suspicious Profile Information
forensics.suspicious_profile.profile_name Availability: Multiple Threats	Suspicious Profile Name
forensics.suspicious_profile.profile_type Availability: Multiple Threats	Suspicious Profile Type
forensics.system_tampering_reasons Availability: Threat Specific	Reasons for the System Tampering detection
forensics.threat_uuid Availability: All Threats	McAfee Internal Field
forensics.time_interval Availability: All Threats	Time that passed since connecting to the network (in seconds).
forensics.type Availability: All Threats	Internal Threat ID

Master Sample JSON

The JSON Body below includes all threat fields of all the threats for both Android and iOS.


```
{
  "severity": 2,
  "event_id": "5acd2c89c6aac430bb6ab3d3",
  "forensics": {
    "time_interval": 944,
    "sideloaded_app_package": "com.McAfee.McAfee MVISION Mobile Application",
    "responses": [
      0
    ],
    "SSID": "Free Wi-Fi",
    "BSSID": "2e:19:8f:f4:42:b3",
    "probabilities": [
      0.4791315793991089,
      0.5208683609962463
    ],
    "os": 1,
    "process_list": [
      {
        "Process Name": "/init",
        "Process ID(PID)": "1",
        "User": "root",
        "Service": "u:r:init:s0",
        "Parent process(PPID)": "0"
      },
      {
        "Process Name": "kthreadd",
        "Process ID(PID)": "2",
        "User": "root",
        "Service": "u:r:kernel:s0",
        "Parent process(PPID)": "0"
      }
    ],
    "attack_time": {
      "$date": 1523395721249
    },
    "close_networks": [
      {
        "capabilities": "[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]",
        "frequency": 2462.0,
        "SSID": "Free Wi-Fi",
        "BSSID": "2e:19:8f:f4:42:b3",
        "level": -47
      },
      {
        "capabilities": "[WPA2-PSK-CCMP][ESS]",
        "frequency": 2412.0,
        "SSID": "ZGuest",
        "BSSID": "c4:13:e2:2b:30:14",
        "level": -46
      }
    ],
    "json_jailbreak_reasons": "[ \"Found SU binary in /sbin/su\" ]",
    "baseline_traceroute": "192.168.12.1 38.96.200.161 154.24.26.113",
```

```
    "captive_portal_before": "<html>\n<head>\n<title>Continue to secure
zone</title></head>\n<body>\n<a href=\"https://demo-device-api.McAfee.com/stest\"><b>Click here
to continue</b></a>\n</body>\n</html>\n",
    "rogue_access_point": {
      "frequency": -1.0,
      "SSID": "\"Planet\"",
      "BSSID": "00:c0:ca:aa:bb:cc"
    },
    "general": [
      {
        "type": "interval",
        "name": "Time Interval",
        "val": "944"
      },
      {
        "name": "Threat Type",
        "val": "Abnormal Process Activity"
      },
      {
        "name": "Device IP",
        "val": "192.168.0.101"
      },
      {
        "name": "Device MAC",
        "val": "78:4b:87:e4:f1:3d"
      },
      {
        "name": "Attacker IP",
        "val": "192.168.0.101"
      },
      {
        "name": "Attacker MAC",
        "val": "78:4b:87:e4:f1:3d"
      },
      {
        "name": "Attacker SSID",
        "val": "192.168.0.101"
      },
      {
        "name": "Attacker BSSID",
        "val": "78:4b:87:e4:f1:3d"
      },
      {
        "name": "Network",
        "val": "Free Wi-Fi"
      },
      {
        "name": "Network BSSID",
        "val": "2e:19:8f:f4:42:b3"
      },
      {
        "name": "Action Triggered",
        "val": "Alert User"
      },
      {
        "name": "Event",
        "val": "File system mounted RW"
      },
      {
        "name": "File Path",
        "val": "/system/"
```

```
      },
      {
        "name": "Change Type",
        "val": "system file"
      },
      {
        "name": "Sideloaded App Developer",
        "val": "O=McAfee"
      },
      {
        "name": "Sideloaded App Name",
        "val": "McAfee MVISION Mobile Application"
      },
      {
        "name": "Sideloaded App Package",
        "val": "com.McAfee.McAfee MVISION Mobile Application"
      },
      {
        "name": "Suspicious Profile Type",
        "val": "Configuration"
      },
      {
        "name": "Suspicious Profile Info",
        "val": "{\n    AuthenticationMethod = SharedSecret;\n    DisconnectOnIdle = 0;\n
DisconnectOnIdleTimer = 0;\n    DisconnectOnSleep = 0;\n    DisconnectOnWake = 1;\n
DisconnectOnWakeTimer = 0;\n    LocalIdentifier = \"IPSEC-zUsers\";\n    LocalIdentifierType =
KeyID;\n    OnDemandEnabled = 0;\n    RemoteAddress = \"zpn-dal.McAfee.com\";\n    SharedSecret =
\"B87C8237-A611-48E6-98BA-8E6E4749AC15.SS\";\n    SharedSecretEncryption = Keychain;\n
XAuthEnabled = 1;\n    XAuthName = \"ios-test\";\n    XAuthPassword = \"B87C8237-A611-48E6-98BA-
8E6E4749AC15.XAUTH\";\n    XAuthPasswordEncryption = Keychain;\n}"
      },
      {
        "name": "Suspicious Profile Name",
        "val": "Setup:/Network/Service/B87C8237-A611-48E6-98BA-8E6E4749AC15/IPSec"
      },
      {
        "name": "External IP",
        "val": "38.96.200.164"
      },
      {
        "name": "Suspected URL",
        "val": "http://www.scbusinc.com/yahoo/d"
      },
      {
        "name": "Process",
        "val": "/init (1) -> /system/bin/debuggerd (289) -> dumpstate (2004) -> logcat (2111) -b
radio -v threadtime -d *:v"
      },
      {
        "name": "Gateway MAC",
        "val": "6c:19:8f:f4:42:b2"
      },
      {
        "name": "Gateway IP",
        "val": "192.168.0.1"
      },
      {
        "name": "IMEI",
        "val": "990004803030133"
      },
      {
```

```
        "type": "json_str",
        "name": "BaseStation",
        "val":
"{\"mnc\":260,\"psc\":510,\"type\":\"WCDMA\",\"cid\":124989444,\"mcc\":310,\"lac\":45991}"
      },
      {
        "type": "json_str",
        "name": "Malware List",
        "val": "{\"Cydia\": 1.0}"
      },
      {
        "type": "json_str",
        "name": "Jailbreak Reasons",
        "val": "Codesign Disabled"
      },
      {
        "name": "DNS before change",
        "val": "8.8.8.8"
      },
      {
        "name": "DNS after change",
        "val": "192.168.0.1"
      },
      {
        "name": "Gateway before change",
        "val": "8.8.8.8"
      },
      {
        "name": "Gateway after change",
        "val": "192.168.0.1"
      },
      {
        "name": "Proxy before change",
        "val": "8.8.8.8"
      },
      {
        "name": "Proxy after change",
        "val": "192.168.0.1"
      },
      {
        "name": "Device Time",
        "val": "04 10 2018 21:16:53"
      },
      {
        "name": "Certificate",
        "val": "*.McAfee.com_CN=Go Daddy Secure Certificate Authority - G2,
OU=http://certs.godaddy.com/repository/, O=\"GoDaddy.com, Inc.\", L=Scottsdale, ST=Arizona,
C=US[0]=-----BEGIN CERTIFICATE-----
\nMIIFKDCCBBCgAwIBAgIJAMEfTAjQKr4lMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYDVQQGEwJVUzEQ\nMA4GA1UECBMHQXJp
m9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEaMBgGA1UEChMRR29EYWRkeS5j\nb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9
ZXJ0cy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5LzEz\nMDEGA1UEAxMqR28gRGFkZHkgU2VjdXJlIENlcnRpZmljYXRlIEF1dG
vcml0eSAtIEcyMB4XDTE1\nMDQxNjE1MDYzOVoXDTE4MDcxNjEyMzIzOVowPTEhMB8GA1UECxMYRG9tYWluIENvbnRyb2wgV
Fs\naWRhdGVkMRgwFgYDVQQDDA8qLnppbXBlcml1bS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw\nggEKAoIBAQDDjs
JM3y8xmPKEbegtFhOufEkKEVnxM7ic+hha6mjHZNODqwW+8z0oj3aDP9jhZF2\nTfXuKHa5bHtbJTlxD4PdLnEOkwa2ocCIC
dCDrobWGYzhrezYQ8MtZ376PxMyv0OAEfCw5dXDvQh\nDTFBP1MdkQwdr3aTFxdDaQVNbkSM+LuHMFZr5XfJe4wKfBU7ML4M
C70sfAcS/gpz3q7aPj89A7X\nzXdAg0KYqoI/+hSHzgPPg+YkhiEK2iV4ph3JdHXL07eGeCOXeYjK7QnwihOiCVPBYysGaor
nsEd\nkMLVdXEvIdPt/1xkGtYZXicNGbvY8kUvQpXZ7Qz6QePbL5XDAgMBAAGjggGxMIIBrTAMBgNVHRMB\nAf8EAjAAMB0G
1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAOBgNVHQ8BAf8EBAMCBaAwNgYD\nVR0fBC8wLTAroCmgJ4YlaHR0cDovL2N
bC5nb2RhZGR5LmNvbS9nZGlnMnMxLTg3LmNybDBTBgNV\nHSAETDBKMEgGC2CGSAGG/W0BBxcBMDkwNwYIKwYBBQUHAgEWK2
0dHA6Ly9jZXJ0aWZpY2F0ZXMu\nZ29kYWRkeS5jb20vcmVwb3NpdG9yeS8wdgYIKwYBBQUHAQEEajBoMCQGCCsGAQUFBzABh
hodHRw\nOi8vb2NzcC5nb2RhZGR5LmNvbS8wQAYIKwYBBQUHMAKGNGh0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29k\nYWRkeS5jb2
```

vcmVwb3NpdG9yeS9nZGlnMi5jcnQwHwYDVR0jBBgwFoAUQMK9J47MNIMwojPX+2yz\n8LQsgM4wKQYDVR0RBCIwIIIPKi56aW
1wZXJpdW0uY29tgg16aW1wZXJpdW0uY29tMB0GA1UdDgQW\nBBQhY/GYtaS0zaaimpDHCWLxT1PB8jANBgkqhkiG9w0BAQsFA
AOCAQEAnOkUf+CpStTA5sVRbcum\n+S0t7XqkKKDjI5A5DqVnHRHN+9o+5b/pgY2GBphi1YsnzGGZ3rUdtCR1i4XFuZMska3I
+xAzP+mn\nziUrlgxXsZCZ2PUAPpb5KiTww0zLOuRZjWXqWT48/T94nQmKGAcYIata4v7dyag30+B8kSVbbuj9\nA19SdyuRl
VyH9X7k2Ot0+8r0Gtx9b2/GD5G/8NsNMfKPhgARp1bNuxrJfzDXg5fu5EsBiKVhWQLJ\n9xcdysKI4FkTTTYfIv3IYVIZdcRN
v9vZZL/umo4Eqc1Mly2DtC1va1j6wqYWGDoJk5vHGOkkZjeh\nvom5cMXTSZUcGHCjjg==\n-----END CERTIFICATE----
-,"
```
      }
    ],
    "captive_portal_after": "<html>\n<head>\n<title>Continue to secure
zone</title></head>\n<body>\n<a href=\"https://demo-device-api.McAfee.com/stest\"><b>Click here
to continue</b></a>\n</body>\n</html>\n",
    "ssl_downgrade_description":
"com.android.org.conscrypt.OpenSSLSocketImpl.startHandshake(OpenSSLSocketImpl.java:448)\ncom.McA
ee.McAfee MVISION Mobile Application.mtdPClientConnection.checkSSLDowngrade(Unknown
Source)\ndalvik.system.NativeStart.run(Native Method)\n",
    "routing_table": [
      {
        "use": 0,
        "netif": "wlan0",
        "refs": 1,
        "destination": "108.177.112.188",
        "flags": "0",
        "gateway": "192.168.0.1"
      },
      {
        "use": 0,
        "netif": "wlan0",
        "refs": 0,
        "destination": "129.42.38.1",
        "flags": "0",
        "gateway": "192.168.0.1"
      }
    ],
    "directory_entries": [
      {
        "hash": "de706e0c44d65d3a9eca570030d9cb8e8ff253511e562052a52a352f680fc10f",
        "permission": "-rw-r--r--",
        "file_name": "/usr/lib/FDRSealingMap.plist",
        "nlink": 1,
        "is_symlink": false,
        "file_size": 6987
      },
      {
        "hash": "32642dc3cab1498af0e7cf9fcb527fb75dc6b6e9128466e4a6668fa9deb789e5",
        "permission": "-rw-r--r--",
        "file_name": "/usr/lib/StandardDMCFiles/N71_Audio.dmc",
        "nlink": 1,
        "is_symlink": false,
        "file_size": 53968
      }
    ],
    "proxy_conf": {
      "ip_after": "192.168.0.7",
      "ip_before": "192.168.0.1"
    },
    "file_system_change": {
      "change_type": 1,
      "event": "File system mounted RW",
      "full_path": "/system/"
    },
```

```
    "ssl_strip_reply": "<html>\n<head>\n<title>Continue to secure zone</title></head>\n<body>\n<a
href=\"http://wwwww.demo-device-api.McAfee.com/stest\"><b>Click here to
continue</b></a>\n</body>\n</html>\n",
    "mitm_traceroute": "192.168.0.106 192.168.12.1 38.96.200.161",
    "dangerzone_nearby_wifi": "ZGuest,zifi",
    "threat_uuid": "4610fdac-a5fb-4f7e-99df-7823ee1f46ad",
    "sample_data":
"0,0,0,0,0,0,0,0,0,76.3494,45.8097,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,78.6986,3.89088,0,0,0,0,0,0,66.3653,1.02778,0,0,0,0,0,0,0,0,3
81747,0,0,0,3.67065,0,0.146826,0.954368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0.954368,0,0.954368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0.146826,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,1,1,0,0,0,1,0,0,0,52,0,0,0,0,0,0,100,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,",
    "network_threat": {
      "net_stat": [
        {
          "Proto": "TCP",
          "Send-Q": "0",
          "Local Address": "192.168.0.101:33504",
          "State": "TIME_WAIT",
          "Foreign Address": "172.217.4.65:443",
          "Recv-Q": "root"
        },
        {
          "Proto": "TCP",
          "Send-Q": "0",
          "Local Address": "192.168.0.101:58933",
          "State": "TIME_WAIT",
          "Foreign Address": "65.61.137.117:80",
          "Recv-Q": "root"
        }
      ],
      "attacker_ip": "192.168.0.101",
      "my_ip": "192.168.0.101",
      "my_mac": "78:4b:87:e4:f1:3d",
      "routing_table": [
        {
          "Use": "0",
          "Netif": "wlan0",
          "Refs": "0",
          "Destination": "129.42.38.1",
          "Flags": "0",
          "Gateway": "192.168.0.1"
        },
        {
          "Use": "1",
          "Netif": "wlan0",
          "Refs": "0",
          "Destination": "13.95.96.176",
          "Flags": "0",
          "Gateway": "192.168.0.1"
        }
      ],
      "gw_ip": "192.168.0.1",
      "delta_route_cache": {
        "table": [
          {
            "ip": "192.168.0.100",
            "gateway": "192.168.0.100"
```

```
          }
        ]
      },
      "interface": "wlan0",
      "attacker_mac": "00:c0:ca:8f:d6:31",
      "basestation":
"{\"mnc\":260,\"psc\":251,\"type\":\"WCDMA\",\"cid\":124989446,\"mcc\":310,\"lac\":45991}",
      "gw_mac": "6c:19:8f:f4:42:b2",
      "arp_tables": {
        "initial": {
          "table": [
            {
              "ip": "192.168.0.1",
              "mac": "6c:19:8f:f4:42:b2"
            },
            {
              "ip": "192.168.0.102",
              "mac": "00:c0:ca:8f:d6:31"
            }
          ]
        },
        "after": {
          "table": [
            {
              "ip": "192.168.0.1",
              "mac": "00:c0:ca:8f:d6:31"
            },
            {
              "ip": "192.168.0.102",
              "mac": "00:c0:ca:8f:d6:31"
            }
          ]
        },
        "before": {
          "table": [
            {
              "ip": "192.168.0.1",
              "mac": "6c:19:8f:f4:42:b2"
            },
            {
              "ip": "192.168.0.102",
              "mac": "00:c0:ca:8f:d6:31"
            }
          ]
        }
      }
    },
    "ssl_mitm_certificate": "*.McAfee.com_CN=Go Daddy Secure Certificate Authority - G2,
OU=http://certs.godaddy.com/repository/, O=\"GoDaddy.com, Inc.\", L=Scottsdale, ST=Arizona,
C=US[0]=-----BEGIN CERTIFICATE-----
\nMIIFKDCCBBCgAwIBAgIJAMEfTAjQKr4lMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYDVQQGEwJVUzEQ\nMA4GA1UECBMHQXJp
m9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEaMBgGA1UEChMRR29EYWRkeS5j\nb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9
ZXJ0cy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5LzEz\nMDEGA1UEAxMqR28gRGFkZHkgU2VjdXJlIENlcnRpZmljYXRlIEF1dG
vcml0eSAtIEcyMB4XDTE1\nMDQxNjE1MDYzOVoXDTE4MDcxNjEyMzIzOVowPTEhMB8GA1UECxMYRG9tYWluIENvbnRyb2wgV
Fs\naWRhdGVkMRgwFgYDVQQDDA8qLnppbXBlcml1bS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw\nggEKAoIBAQDDjs
JM3y8xmPKEbegtFhOufEkKEVnxM7ic+hha6mjHZNODqwW+8z0oj3aDP9jhZF2\nTfXuKHa5bHtbJTlxD4PdLnEOkwa2ocCIC
dCDrobWGYzhrezYQ8MtZ376PxMyv0OAEfCw5dXDvQh\nDTFBP1MdkQwdr3aTFxdDaQVNbkSM+LuHMFZr5XfJe4wKfBU7ML4M
C70sfAcS/gpz3q7aPj89A7X\nzXdAg0KYqoI/+hSHzgPPg+YkhiEK2iV4ph3JdHXL07eGeCOXeYjK7QnwihOiCVPBYysGaor
nsEd\nkMLVdXEvIdPt/1xkGtYZXicNGbvY8kUvQpXZ7Qz6QePbL5XDAgMBAAGjggGxMIIBrTAMBgNVHRMB\nAf8EAjAAMB0G
1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAOBgNVHQ8BAf8EBAMCBaAwNgYD\nVR0fBC8wLTAroCmgJ4YlaHR0cDovL2N
bC5nb2RhZGR5LmNvbS9nZGlnMnMxLTg3LmNybDBTBgNV\nHSAETDBKMEgGC2CGSAGG/W0BBxcBMDkwNwYIKwYBBQUHAgEWK2
```

0dHA6Ly9jZXJ0aWZpY2F0ZXMu\nZ29kYWRkeS5jb20vcmVwb3NpdG9yeS8wdgYIKwYBBQUHAQEEajBoMCQGCCsGAQUFBzABhh
hodHRw\nOi8vb2NzcC5nb2RhZGR5LmNvbS8wQAYIKwYBBQUHMAKGNGh0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29k\nYWRkeS5jb2(
vcmVwb3NpdG9yeS9nZGlnMi5jcnQwHwYDVR0jBBgwFoAUQMK9J47MNIMwojPX+2yz\n8LQsgM4wKQYDVR0RBCIwIIIPKi56aW
1wZXJpdW0uY29tgg16aW1wZXJpdW0uY29tMB0GA1UdDgQW\nBBQhY/GYtaS0zaaimpDHCWLxT1PB8jANBgkqhkiG9w0BAQsFA
AOCAQEAnOkUf+CpStTA5sVRbcum\n+S0t7XqkKKDjI5A5DqVnHRHN+9o+5b/pgY2GBphi1YsnzGGZ3rUdtCR1i4XFuZMska3I
+xAzP+mn\nziUrlgxXsZCZ2PUAPpb5KiTww0zLOuRZjWXqWT48/T94nQmKGAcYIata4v7dyag30+B8kSVbbuj9\nA19SdyuRI
VyH9X7k2Ot0+8r0Gtx9b2/GD5G/8NsNMfKPhgARp1bNuxrJfzDXg5fu5EsBiKVhWQLJ\n9xcdysKI4FkTTTYfIv3IYVIZdcRM
v9vZZL/umo4Eqc1Mly2DtC1va1j6wqYWGDoJk5vHGOkkZjeh\nvom5cMXTSZUcGHCjjg==\n-----END CERTIFICATE----
-",
    "android_compatibility_check_response":
"eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlFaWpDQ0EzS2dBd0lCQWdJSVlrWW81RjBnODZrd0RRWUpLb1pJaHZjTkFRRUx(
UUF3VkRFTE1Ba0dBMVVFQmhNQ1ZWTXhIakFjQmdOVkJBb1RGVWR2YjJkc1pTQlVjblZ6ZENCVFpYSjJhV05sY3pFbE1DTUdBM
VVFQXhNY1IyOXZaMnhsSUVsdWRHVnlibVYwSUVGMWRHaHZjbWwwZVNCSE16QWVGdzB4TnpFeU1EUXhNekU0TkROYUZ3MHhPRE
V5TURNd01EQXdNREJhTUd3eEN6QUpCZ05WQkFZVEFsVlRNUk13RVFZRFZRUUlEQXBEWVd4cFptOXlibWxoTVJZd0ZBWURWUVE
IREExTmIzVnVkR0ZwYmlCV2FXVjNNUk13RVFZRFZRUUtEQXBIYjI5bmJHVWdTVzVqTVJzd0dRWURWUVFEREJKaGRIUmxjM1FI
WVc1a2NtOXBaQzVqYjIwd2dnRWlNQTBHQ1NxR1NJYjNEUUVCQVFVQUE0SUJEd0F3Z2dFS0FvSUJBUUNVajh3WW9QaXhLYmJWC
HNnWWd2TVRmWCtkSXNGVE9rZ0tPbGhUMGkwYmNERlpLMnJPeEpaMnVTTFNWaFl2aXBaTkUzSEpRWXV1WXdGaml5K3lrZmF0QU
dTalJ6RjFiMzF1NDMvN29HNWpNaDNTMzdhbHdqVWI4Q1dpVHhvaXBWT1l3S0t6dVV5a3FFQ3RqbGhKNEFrV2FEUytaeEtFcU
hZTl0bkNnZUhsbFpFL09SZ2VNYXgyWE5Db0g2c3JURVJja3NqelpackFXeEtzZGZ2VnJYTnpDUjlEeFZBU3VJNkx6d2g4RFNs
MkVPb2tic2FuWisrL0pxTWVBQkZmUHdqeXdyYjBwckVVeTBwYWVWc3VkKzBwZWV4Sy81K0U2a3BZR0s0WksybmtvVkx1Z0U1c
GFIckFqODNRK1BPYmJ2T3pXY0ZrcG5WS3lqbzZLUUFtWDZXSkFnTUJBQUdqZ2dGR01JSUJRakFUQmdOVkhTVUVEREFLQmdncl
JnRUZCUWNEQVRBZEJnTlZIUkVFRmpBVWdoSmhkSFJsYzNRdVlXNWtjbTlwWkM1amIyMHdhQVlJS3dZQkJRVUhBUUVFWERCYU1
DMEdDQ3NHQVFVRkJ6QUNoaUZvZEhSd09pOHZjR3RwTG1kdmIyY3ZaM055TWk5SFZGTkhTVUZITXk1amNuUXdLUVlJS3dZQkJR
VUhNQUdHSFdoMGRIQTZMeTl2WTNOd0xuQnJhUzVuYjI5bkwwZFVVMGRKUVVjek1CMEdBMVVkRGdRV0JCUUc4SXJRdEZSNkNVU
2tpa2IzYWltc20yNmNCVEFNQmdOVkhSTUJBZjhFQWpBQU1COEdBMVVkSXdRWU1CYUFGSGZDdUZDYVozWjJzUzNDaHRDRG9INm
1mcnBMTUNFR0ExVWRJQVFhTUJnd0RBWUtLd1lCQkFIV2VRSUZBekFJQmdabmdRd0JBZ0l3TVFZRFZSMGZCQ293S0RBbW9DU2(
Jb1lnYUhSMGNEb3ZMMk55YkM1d2Eya3VaMjl2Wnk5SFZGTkhTVUZITXk1amNtd3dEUVlKS29aSWh2Y05BUUVMQlFBRGdnRUJF
Ri9Sek5uQzVEekJVQnRuaDJudEpMV0VRaDl6RWVGWmZQTDlRb2tybEFvWGdqV2dOOHBTUlUxbFZHSXB0ek14R2h5My9PUlJaV
GE2RDJEeThodkNEckZJMytsQ1kwMU1MNVE2WE5FNVJzMmQxUmlacE1zekQ0S1FaTkczaFowQkZOUS9janJDbUxCT0dLa0VVMW
RtQVhzRkpYSmlPcjJDTlRCT1R1OUViTFdoUWZkQ0YxYnd6eXUrVzZiUVN2OFFEbjVPZE1TL1BxRTFkRWdldC82RUlSQjc2MUt
mWlErL0RFNkxwM1RyWlRwT0ZERGdYaCtMZ0dPc3doRWxqOWMzdlpIR0puaGpwdDhya2Jpci8ydUxHZnhsVlo0SzF4NURSTjBQ
VUxkOXlQU21qZythajErdEh3STFtUW1aVlk3cXZPNURnaE94aEpNR2x6NmxMaVptem9nPSIsIk1JSUVYRENDQTBTZ0F3SUJB
0lOQWVPcE1CejhjZ1k0UDVwVEhUQU5CZ2txaGtpRzl3MEJBUXNGQURCTU1TQXdIZ1lEVlFRTEV4ZEhiRzlpWVd4VGFXZHVJR
p2YjNRZ1EwRWdMU0JTTWpFVE1CRUdBMVVFQ2hNS1IyeHZZbUZzVTJsbmJqRVRNQkVHQTFVRUF4TUtSMnh2WW1Gc1UybG5iak
lRncweE56QTJNVFV3TURBd05ESmFGdzB5TVRFeU1UVXdNREF3TkRKYU1GUXhDekFKQmdOVkJBWVRBbFZUTVI0d0hBWURWUVFI
RXhWSGIyOW5iR1VnVkhKMWMzUWdVMlZ5ZG1salpYTXhKVEFqQmdOVkJBTVRIRWR2YjJkc1pTQkpiblJsY201bGRDQkJkWFJvY
jNKcGRIa2dSek13Z2dFaU1BMEdDU3FHU0liM0RRRUJBUVVBQTRJQkR3QXdnZ0VLQW9JQkFRREtVa3ZxSHYvT0pHdW8ybklZU
5WV1hRNUlXaTAxQ1haYXo2VElITEdwL2xPSis2MDAvNGhibjd2bjZBQUIzRFZ6ZFFPdHM3RzVwSDBySm5uT0ZVQUs3MUc0bnp
LTWZIQ0dVa3NXL21vbmErWTJlbUpRMk4rYWljd0pLZXRQS1JTSWdBdVBPQjZBYWhoOEhiMlhPM2g5UlVrMlQwSE5vdUIyVnp4
b01YbGt5VzdYVVI1bXc2SmtMSG5BNTJYRFZvUlRXa050eTVvQ0lOTHZHbW5Sc0oxem91QXFZR1ZRTWMvN3N5Ky9FWWhBTHJWS
kVBOEtidHlYK3I4c253VTVDMWhVcndhVzZNV09BUmE4cUJwTlFjV1RrYUllb1l2eS9zR0lKRW1qUjB2RkV3SGRwMWNTYVdJc
YvNGc3Mm43T3FYd2ZpbnU3WllXOTdFZm9PU1FKZUF6QWdNQkFBR2pnZ0V6TUlJQkx6QU9CZ05WSFE4QkFmOEVCQU1DQVlZd0
RWURWUjBsQkJZd0ZBWUlLd1lCQlFVSEF3RUdDQ3NHQVFVRkJ3TUNNQklHQTFVZEV3RUIvd1FJTUFZQkFmOENBUUF3SFFZRFZS
ME9CQllFRkhmQ3VGQ2FaM1oyc1MzQ2h0Q0RvSDZtZnJwTE1COEdBMVVkSXdRWU1CYUFGSnZpQjFkbkhCN0FhZ2JlV2JTYUxkI
2NHWVl1TURVR0NDc0dBUVVGQndFQkJDa3dKekFsQmdnckJnRUZCUWN3QVlZWmFIUjBjRG92TDI5amMzQXVjR3RwTG1kdmIyY3
ZaM055TWpBeUJnTlZIUjhFS3pBcE1DZWdKYUFqaGlGb2RIUndPaTh2WTNKc0xuQnJhUzVuYjI5bkwyZHpjakl2WjNOeU1pNWp
jbXd3UHdZRFZSMGdCRGd3TmpBMEJnWm5nUXdCQWdJd0tqQW9CZ2dyQmdFRkJRY0NBUlljYUhSMGNITTZMeTl3YTJrdVoyOXZa
eTl5WlhCdmMybDBiM0o1THpBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQUhMZUpsdVJUN2J2czI2Z3lBWjhzbzgxdHJVSVNkN
080NXNrRFVtQWdlMWNueGhHMVAyY05tU3hiV3NvaUN0MmV1eDlMU0QrUEFqMkxJWVJGSFczMS82eG9pYzFrNHRiV1hrRENqaX
IzN3hUVE5xUkFNUFV5RlJXU2R2dCtubFBxd25iOE9hMkkvbWFTSnVrY3hEak5TZnBEaC9CZDFsWk5nZGQvOGNMZHNFMyt3eXF
1Zko5dVhPMWlRcG5oOXpidUZJd3NJT05HbDFwM0E4Q2d4a3FJL1VBaWgzSmFHT3FjcGNkYUNJemtCYVI5dVlRMVg0azJWZzVF
UFJMb3V6Vnk3YThJVms2d3V5NnBtK1Q3SFQ0TFk4aWJTNUZFWmxmQUZMU1c4TndzVno5U0JLMlZxbjFOMFBJTW41eEE2TlpWY
zdvODM1RExBRnNoRVdmQzdUSWUzZz09Il19.eyJub25jZSI6ImFJbzZQa3BzdHVUd3daYitTTk9HT3F5ZGJmbjYyeXNmeDFQk
WtWcXd2RUU9IiwidGltZXN0YW1wTXMiOjE1MjM0MDI5NTg1NjYsImFwa1BhY2thZ2VOYW1lIjoiY29tLnppbXBlcml1bS56aX
BzIiwiYXBrRGlnZXN0U2hhMjU2IjoiK2pZWDlvckNGSWtZN3hsSGs3MDhMdmtRU09KNXM3S1QwdlVpTUJTcTZPTT0iLCJjdHN
Qcm9maWxlTWF0Y2giOmZhbHNlLCJhcGtDZXJ0aWZpY2F0ZURpZ2VzdFNoYTI1NiI6WyJxNXRKN09TdGRNYUYwUGN3R3ZiYXMy
eUd1U1ZaOEpyWVF1WHQ4MW1rdHg4PSJdLCJiYXNpY0ludGVncml0eSI6ZmFsc2UsImFkdmljZSI6IlJFU1RPUkVfVE9fRkFDV
E9SWV9ST00ifQ.kRgYAPflVp6Suo9ueOJTbkIzGxk62f5ozB--tdOe1BmZuWtYn23zr-
JJrZnh1xn6X3bC7cYuVT7vjg_Rj3dg4bn3W80imI6ZguXfdXZnlDI7ujbwWfAn4cdNHmbCP-wkWMnc0-
Xa4m7XjZCGFAKGeTHkcw90LgkVYO-TAktw_5FcPymnIPyxHXXQ39MDvUvwXBr-
mSIeNLoLNk27RGLG75jpqpN5S00lGV9job5dqykAuY-

nEUvWmjaYBl45HgdxRNRtABKNyX2d9asjCFLhp8BzsxpWuMQAAwmfDlAYMackrbTHKI5OZMxsQlKWCIMk24QluoXbbGtqJpH
D76lmw",
    "sideloaded_app_name": "McAfee MVISION Mobile Application",
    "suspicious_profile": {
      "profile_information": "{\n   AuthenticationMethod = SharedSecret;\n   DisconnectOnIdle =
0;\n   DisconnectOnIdleTimer = 0;\n   DisconnectOnSleep = 0;\n   DisconnectOnWake = 1;\n
DisconnectOnWakeTimer = 0;\n   LocalIdentifier = \"IPSEC-zUsers\";\n   LocalIdentifierType =
KeyID;\n   OnDemandEnabled = 0;\n   RemoteAddress = \"zpn-dal.McAfee.com\";\n   SharedSecret =
\"B87C8237-A611-48E6-98BA-8E6E4749AC15.SS\";\n   SharedSecretEncryption = Keychain;\n
XAuthEnabled = 1;\n   XAuthName = \"ios-test\";\n   XAuthPassword = \"B87C8237-A611-48E6-98BA-
8E6E4749AC15.XAUTH\";\n   XAuthPasswordEncryption = Keychain;\n}",
      "profile_name": "Setup:/Network/Service/B87C8237-A611-48E6-98BA-8E6E4749AC15/IPSec",
      "profile_type": 1
    },
    "system_tampering_reasons": "SELinux state change : 0",
    "_id": {
      "$oid": "5acd2c8a70b7705a570dd76d"
    },
    "type": 10,
    "sideloaded_app_developer": "iPhone Distribution: McAfee, Inc.",
    "host_attack": {
      "malware_matches": [
        {
          "signatures": [
            {
              "type": 0,
              "hash": "45F86E5027495DC33D168F4F4704779C",
              "size": 90311
            },
            {
              "type": 2,
              "hash": "B48B1E51097ADE6DB1EB15A7DFBC0B81",
              "size": 33
            },
            {
              "type": 2,
              "hash": "4F5B0D6B9BCD31EDC7628DEEF9978560",
              "size": 27
            },
            {
              "type": 2,
              "hash": "0BF2BC52BFCC27A2B24F1C3E97DE69BA",
              "size": 31
            },
            {
              "type": 2,
              "hash": "15E39F90DA03CC20E525CE84FE0FC2BA",
              "size": 31
            },
            {
              "type": 2,
              "hash": "03F3625328A7A76A5C330D99D57EE261",
              "size": 24
            }
          ],
          "score": 6.0,
          "name": "Trojan.Droidkungfu/2"
        }
      ],
      "detected_locally": **true**,
      "process": "/init (1) -> /system/bin/debuggerd (289) -> dumpstate (2004) -> logcat (2111) -

b radio -v threadtime -d *:v",
      "malware_detection_source": 0,
      "filename": "/data/app/com.tebs3.cuttherope-1/base.apk",
      "file_hash": "45f86e5027495dc33d168f4f4704779c",
      "application": "com.tebs3.cuttherope",
      "malware_threat_name": "Trojan.Droidkungfu/2",
      "is_blacklisted": **true**,
      "is_malicious": **false**,
      "malware_scan_category": 1,
      "suspected_url": "http://www.scbusinc.com/yahoo/d",
      "daemon_minflt": [
        64530,
        64530,
        64530,
        65981,
        66711,
        66752,
        67231,
        68632,
        70771
      ],
      "process_pid": 2111,
      "daemon_rss": [
        1513,
        1507,
        1498,
        1931,
        1983,
        1986,
        2334,
        3720,
        5898
      ],
      "info_before": {
        "user_id": "2000",
        "selinux_context": "u:r:s_dumpstate:s0"
      },
      "info_after": {
        "user_id": "2000",
        "selinux_context": "u:r:s_dumpstate:s0"
      }
    },
    "app_tampering_reasons": "MobileSubstrate code injection library detected",
    "stagefright_vulnerability_report": "{\"CVE-2015-3828\":false,\"CVE-2015-3827\":true,\"CVE-2015-3829\":true,\"CVE-2015-6575-2\":true,\"CVE-2015-6602\":true,\"CVE-2015-1538\":true,\"CVE-2015-6575-3\":true,\"CVE-2015-3876\":false,\"CVE-2015-6575-1\":true,\"CVE-2015-3824\":true,\"CVE-2015-3864\":true}",
    "severity": 2
  },
  "mitigated": "True",
  "location": {
    "state_name": "Texas",
    "source": 4,
    "p": [
      -99.9018131,
      31.9685988
    ],
    "country_name": "United States",
    "previous_sample": {
      "p": [
        -96.84407620148978,

```
        32.92587490052974
      ],
      "time": {
        "$date": 1523407557000
      }
    },
    "exact": false,
    "sampled_time": {
      "$date": 1523393223000
    },
    "accuracy": 2
  },
  "eventtimestamp": "2018-04-10 21:28:44.201372+00:00",
  "user_info": {
    "employee_name": "Jane Carem",
    "user_role": "End User",
    "user_email": "jane.carem@zmdemo.com",
    "user_group": "Default Group"
  },
  "device_info": {
    "device_time": "2018-04-10 21:28:44.201372+00:00",
    "tag1": "",
    "tag2": "",
    "app": "McAfee MVISION Mobile Application",
    "operator": "Sprint",
    "imei": "990004803030133",
    "os": "Android",
    "jailbroken": false,
    "os_version": "5.0",
    "model": "SM-G900V",
    "app_version": "4.3.3",
    "type": "kltevzw"
  },
  "threat": {
    "story": "Detected Abnormal Process Activity while connected to Free Wi-Fi.  Responded with
Alert User.",
    "name": "Abnormal Process Activity",
    "general": {
      "time_interval": "944",
      "device_time": "04 10 2018 21:16:53",
      "threat_type": "Abnormal Process Activity",
      "device_ip": "192.168.0.101",
      "device_mac": "78:4b:87:e4:f1:3d",
      "gateway_ip": "192.168.0.1",
      "gateway_mac": "6c:19:8f:f4:42:b2",
      "network": "Free Wi-Fi",
      "network_bssid": "2e:19:8f:f4:42:b3",
      "external_ip": "38.96.200.164",
      "basestation":
"{\"mnc\":260,\"psc\":510,\"type\":\"WCDMA\",\"cid\":124989444,\"mcc\":310,\"lac\":45991}",
      "action_triggered": "Alert User",
      "attacker_ip": "192.168.1.8",
      "attacker_mac": "6c:19:8f:f4:42:b2",
      "attacker_ssid": "\"Planet\"",
      "attacker_bssid": "00:c0:ca:aa:bb:cc",
      "process": "/init (1) -> /system/bin/debuggerd (289) -> dumpstate (2004) -> logcat (2111) -
b radio -v threadtime -d *:v",
      "certificate": "*.McAfee.com_CN=Go Daddy Secure Certificate Authority - G2,
OU=http://certs.godaddy.com/repository/, O=\"GoDaddy.com, Inc.\", L=Scottsdale, ST=Arizona,
C=US[0]=-----BEGIN CERTIFICATE-----
\nMIIFKDCCBBCgAwIBAgIJAMEfTAjQKr4lMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYDVQQGEwJVUzEQ\nMA4GA1UECBMHQXJp
```

m9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEaMBgGA1UEChMRR29EYWRkeS5j\nb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9
ZXJ0cy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5LzEz\nMDEGA1UEAxMqR28gRGFkZHkgU2VjdXJlIENlcnRpZmljYXRlIEF1dG
vcml0eSAtIEcyMB4XDTE1\nMDQxNjE1MDYzOVoXDTE4MDcxNjEyMzIzOVowPTEhMB8GA1UECxMYRG9tYWluIENvbnRyb2wgVr
Fs\naWRhdGVkMRgwFgYDVQQDDA8qLnppbXBlcml1bS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw\nggEKAoIBAQDDjs
JM3y8xmPKEbegtFhOufEkKEVnxM7ic+hha6mjHZNODqwW+8z0oj3aDP9jhZF2\nTfXuKHa5bHtbJTlxD4PdLnEOkwa2ocCIC
dCDrobWGYzhrezYQ8MtZ376PxMyv0OAEfCw5dXDvQh\nDTFBP1MdkQwdr3aTFxdDaQVNbkSM+LuHMFZr5XfJe4wKfBU7ML4M
C70sfAcS/gpz3q7aPj89A7X\nzXdAg0KYqoI/+hSHzgPPg+YkhiEK2iV4ph3JdHXL07eGeCOXeYjK7QnwihOiCVPBYysGaor
nsEd\nkMLVdXEvIdPt/1xkGtYZXicNGbvY8kUvQpXZ7Qz6QePbL5XDAgMBAAGjggGxMIIBrTAMBgNVHRMB\nAf8EAjAAMB0G
1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAOBgNVHQ8BAf8EBAMCBaAwNgYD\nVR0fBC8wLTAroCmgJ4YlaHR0cDovL2N
bC5nb2RhZGR5LmNvbS9nZGlnMnMxLTg3LmNybDBTBgNV\nHSAETDBKMEgGC2CGSAGG/W0BBxcBMDkwNwYIKwYBBQUHAgEWK2
0dHA6Ly9jZXJ0aWZpY2F0ZXMu\nZ29kYWRkeS5jb20vcmVwb3NpdG9yeS8wdgYIKwYBBQUHAQEEajBoMCQGCCsGAQUFBzABh
hodHRw\nOi8vb2NzcC5nb2RhZGR5LmNvbS8wQAYIKwYBBQUHMAKGNGh0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29k\nYWRkeS5jb2
vcmVwb3NpdG9yeS9nZGlnMi5jcnQwHwYDVR0jBBgwFoAUQMK9J47MNIMwojPX+2yz\n8LQsgM4wKQYDVR0RBCIwIIIPKi56a
1wZXJpdW0uY29tgg16aW1wZXJpdW0uY29tMB0GA1UdDgQW\nBBQhY/GYtaS0zaaimpDHCWLxT1PB8jANBgkqhkiG9w0BAQsF
AOCAQEAnOkUf+CpStTA5sVRbcum\n+S0t7XqkKKDjI5A5DqVnHRHN+9o+5b/pgY2GBphi1YsnzGGZ3rUdtCR1i4XFuZMska3
+xAzP+mn\nziUrlgxXsZCZ2PUAPpb5KiTww0zLOuRZjWXqWT48/T94nQmKGAcYIata4v7dyag30+B8kSVbbuj9\nA19SdyuR
VyH9X7k2Ot0+8r0Gtx9b2/GD5G/8NsNMfKPhgARp1bNuxrJfzDXg5fu5EsBiKVhWQLJ\n9xcdysKI4FkTTTYfIv3IYVIZdcR
v9vZZL/umo4Eqc1Mly2DtC1va1j6wqYWGDoJk5vHGOkkZjeh\nvom5cMXTSZUcGHCjjg==\n-----END CERTIFICATE----
-,",
"malware_list": "{\"Cydia\": 1.0}",
"suspicious_profile_name": "Setup:/Network/Service/B87C8237-A611-48E6-98BA-8E6E4749AC15/IPSec",
"suspicious_profile_info": "{\n   AuthenticationMethod = SharedSecret;\n   DisconnectOnIdle = 0;\n   DisconnectOnIdleTimer = 0;\n   DisconnectOnSleep = 0;\n   DisconnectOnWake = 1;\n   DisconnectOnWakeTimer = 0;\n   LocalIdentifier = \"IPSEC-zUsers\";\n   LocalIdentifierType = KeyID;\n   OnDemandEnabled = 0;\n   RemoteAddress = \"zpn-dal.McAfee.com\";\n   SharedSecret = \"B87C8237-A611-48E6-98BA-8E6E4749AC15.SS\";\n   SharedSecretEncryption = Keychain;\n   XAuthEnabled = 1;\n   XAuthName = \"ios-test\";\n   XAuthPassword = \"B87C8237-A611-48E6-98BA-8E6E4749AC15.XAUTH\";\n   XAuthPasswordEncryption = Keychain;\n}",
"suspicious_profile_type": "Configuration",
"imei": "990004803030133",
"file_hash": "45f86e5027495dc33d168f4f4704779c",
"jailbreak_reasons": "Codesign Disabled",
"sideloaded_app_name": "McAfee MVISION Mobile Application",
"sideloaded_app_package": "com.McAfee.McAfee MVISION Mobile Application",
"sideloaded_app_developer": "O=McAfee",
"gateway_before_change": "192.168.0.1",
"dns_before_change": "8.8.8.8",
"proxy_after_change": "nskz.xks",
"gateway_after_change": "192.168.0.7",
"dns_after_change": "192.168.0.1",
"suspected_url": "http://www.scbusinc.com/yahoo/d",
"event": "File system mounted RW",
"file_path": "/system/",
"stagefright_vulnerability_report": "{\"CVE-2015-3828\":false,\"CVE-2015-3827\":true,\"CVE-2015-3829\":true,\"CVE-2015-6575-2\":true,\"CVE-2015-6602\":true,\"CVE-2015-1538\":true,\"CVE-2015-6575-3\":true,\"CVE-2015-3876\":false,\"CVE-2015-6575-1\":true,\"CVE-2015-3824\":true,\"CVE-2015-3864\":true}",
"change_type": "system file"
}
}
}

Appendix A – Sample Pull Script

```
#!/usr/bin/env bash
#: Title : Customer Splunk curl syslog retrieval
#: Date : 2016-03-30
#: Author : McAfee
#: Version : 2.1
#: Description : Activate syslog forwarder on files to customer receiver

#Add a chrone job to run this file once a minute, Example:
# 1 * * * * /home/ubuntu/syslog_curl.sh

#Security paramaters: Acquire these from McAfee Support: support@McAfee.com
client_id='UP9Vg7ugzUVQQBQs5DSib8zPC4dC4E48kR1af3lB'
client_secret='1aDFBanlG56yOZCC2hG6BQzOnzsUw07jLWaOYbRpi7WAp1pIq6Gue87SGnQ1d65sAYSXZvzq7odcri9E
qI2xGJom8vbl5xG5dJhWpeBStbIwMl1J2PjNJu5hd2TvXX2m'
system_token_encoded='YWlnLIlLYw=='

#Where to get the auth token and the McAfee MVISION Mobile Console logs
authhost='demo-token.McAfee.com'
McAfee MVISION Mobile ConsoleHost='demo-console.McAfee.com'

#Location where we want the data to reside and the start of the filename
destinationDir='/var/log/McAfee_spm'
output_file_prefix='json_'

function parse_json()
{
    echo $1 | \
    sed -e 's/[{}]/''/g' | \
    sed -e 's/", "/'\",\"'/g' | \
    sed -e 's/" ,"/'\",\"'/g' | \
    sed -e 's/" , "/'\",\"'/g' | \
    sed -e 's/","/'\"---SEPERATOR---\"'/g' | \
    awk -F=':' -v RS='---SEPERATOR---' "\$1~/\"$2\"/ {print}" | \
    sed -e "s/\"$2\":://" | \
    tr -d "\n\t" | \
    sed -e 's/\\"/"/g' | \
    sed -e 's/\\\\/\\/g' | \
    sed -e 's/^[ \t]*//g' | \
    sed -e 's/^"//'  -e 's/"$//'
}

if [ ! -d "$destinationDir" ]; then
      echo "Directory does not exist: " $destinationDir " please create this directory and
restart."
      exit 1
fi

echo "getting security access token.."
json_with_access_token=$(curl -vv https://${authhost}/oauth2/token/ --data
"grant_type=client_credentials&client_id=$client_id&client_secret=$client_secret")
access_token=$(parse_json "${json_with_access_token}" access_token)

echo $json_with_access_token
echo ACCESS TOKEN
echo $access_token
if [ -z "$access_token" ]; then
    echo "ERROR!! could not get access token, response was probably invalid"
```

```
    rm -f $destinationDir/syslog_access_token
    exit -1
fi

echo $access_token > $destinationDir/syslog_access_token



# severity: 0 = Normal, 1=Low, 2=Elevated, 3=Critical

# Below example pulls data for Severity 2,3 ( Elevated, Critical only )

# $system_token_encoded?severity=3&severity=2

# Default level=verbose

# $system_token_encoded?level=concise


echo "getting syslogs.."

prefilename="$destinationDir/$output_file_prefix`date +'%m%d%y%H%M%S'`-pre.log"
status_code=$(curl -k -s -f -H 'Authorization: Bearer '$access_token'' https://${McAfee MVISION
Mobile ConsoleHost}/seclog/$system_token_encoded?level=concise\&severity=3 -o $prefilename  -w
"%{http_code}")

echo STATUS CODE
echo $status_code

if test -f "$prefilename"; then
   filename="$destinationDir/$output_file_prefix`date +'%m%d%y%H%M%S'`.log"
   touch $filename
   while read -r line; do
        test="$( cut -d '{' -f 2- <<< "$line" )"
        echo "{"$test >> $filename
   done <$prefilename
   rm -f $prefilename
fi

if [ "$status_code" =  200 ]
then
    find ${destinationDir}/${output_file_prefix}*.log -mtime 7 | xargs rm
else
    echo 'ERROR!! got status code: ' $status_code 'from the server..'
fi
```