



Zimperium zConsole

Threat Reference Guide

zConsole Release 4.33.x

May 2021

Copyright © 2021, Zimperium®, Inc. and/or its affiliates. All rights reserved.

This document, as well as the software described in it, is furnished under license. The information in this manual may only be used in accordance with the terms of the license. This document should not be reproduced, stored, or transmitted in any form, except as permitted by the license or by the express permission of Zimperium, Inc.

All other marks and names mentioned herein may be trademarks or trade names of their respective companies.

Table of Contents

Preface	4
Audience	4
Related Documentation	4
New Features	4
Overview	5
Threat Policy	5
Threat Information	6
Threat List	7
Threat List Legend	27

Preface

This guide details the list of threats in the zConsole. The threats are managed on the **Policy** page of zConsole. This document includes information on which threats are supported on Android and iOS. In addition, the guide details the threats supported in the zIPS application and in the zDefend SDK framework.

This document assumes an overall knowledge of Zimperium terms. For more overview information see the “*Zimperium zConsole Configuration Guide*.”

Audience

The intended audience for this guide is zConsole system administrators and zDefend SDK developers. The zConsole application provides threat protection to mobile devices. The system administrator sets policies for threats, and also monitors and manages threats detected. Developers often need a list of threats to integrate with an MDM or to build a mobile application using the zDefend SDK framework.

Related Documentation

Additional Zimperium documents are located on the Customer Support Portal at the website: <http://support.zimperium.com>

New Features

Refer to the “*Zimperium zConsole Release Notes*” document for the list of new features in this release.

Overview

Mobile devices are found everywhere today. They represent an opportunity for malicious actors who are looking to find new ways to gain access to corporate environments. Although corporate environments may have protection from viruses and malicious code on servers, desktops, and laptops, mobile devices are increasingly the new frontier that is being colonized by hackers.

This document provides information on the threat classifications. These threat classifications are presented in the zConsole **Policy** page where system administrators can set severity levels and the desired actions to notify for threats and mitigate actions to the threats.

Threat Policy

The Threat Policy defines the zIPS actions when detecting an event. This is managed on the **Policy** page in the zConsole. Among the options are the following:

- Enable or disable detection of a specific threat classification
- Alert the user or not
- Define the text of the alert
- Define the protection actions to take, such as local at the device or MDM related
- Define if an email, SMS text, or both are to be sent to the logged-in administrator

When done modifying these options, the policies are deployed to the logged-in zIPS devices. See the *“Zimperium zConsole Configuration Guide”* for more information on the v4 zConsole functionality. See the online documentation for the zDefend console.




Threat Information


The threat table lists the threats that are displayed on the zConsole **Policy** page. The columns include:




- **Threat Name:** This is the name of the threat. The table is in alphabetical order by threat name.
- **Threat Description:** This is a description of the threat, followed by the vector for the threat, the threat tag, and the MITRE tactics for each threat, if applicable. The list of vector values is Device (Host), Malware, and Network. The MITRE tactic information is available in the zConsole when you select the information icon. See the “*Zimperium zConsole Configuration Guide*” for more information about vectors and MITRE tactics.
- **Risk or Threat:** This indicates if the threat is a potential risk or an actual threat.
- **Severity Default:** This is the default severity for the threat, for example, Low, Normal, Elevated, or Critical.
- **Android OS:** This column indicates if the threat is supported on an Android device.
- **Apple OS:** This column indicates if the threat is supported on an iOS device.
- **Chrome OS:** This column indicates if the threat is supported on a Chrome OS device.
- **zIPS:** This column indicates if the threat is supported in the zIPS application. Some entries have the zIPS release number in parentheses, indicating in what release it is supported.
- **zDefend SDK:** This column indicates if the threat can be returned by the zDefend SDK framework. Some entries have the zDefend SDK release number in parentheses, indicating in what release it is supported.
- **Threat Identifiers:** This column has two internal identifiers values for a threat. The text identifier value followed by the numerical identifier value. These are used by zDefend SDK users in building their own apps.




***Note:** The items marked with the letter “a” with notation [a] indicate that Hotspot Helper is required for iOS functionality support. Other threats have letters in square brackets for additional notes with the legend at the end of the threat list table. See [“Threat List Legend”](#) for the legend list.*




Threat List




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Abnormal Process Activity	Detected abnormal activity. Your device is being monitored for any attacks. Vector: Device Tag: host.process.activity MITRE Tactics: Execution , Persistence , Impact	Risk	Elevated	Yes (OS<=6 & Knox >= 3.4+)	Jailbroken Devices Only	Yes	Yes	Yes	ABNORMAL_PROCESS_ACTIVITY, 10
Always-on VPN App Set	An app has been configured as an always-on VPN on this device. The app may monitor all communications the device makes to the Internet. Vector: Device Tag: host.always_on_vpn_app MITRE Tactics: Collection , Exfiltration , Network Effects	Risk	Elevated	Yes	---	Yes	Yes (4.8)	Yes (4.8)	ALWAYS_ON_VPN_APP_SET, 87
Android Debug Bridge (ADB) Apps Not Verified	Apps installed via ADB are not required to be verified. This may allow malicious apps to be installed on the device. Vector: Network Tag: host.adb_apps_not_verified MITRE Tactics: Initial Access , Privilege Escalation , Persistence , Credential Access , Lateral Movement , Collection , Exfiltration	Risk	Elevated	Yes	---	Yes	Yes (4.8)	Yes (4.8)	ANDROID_DEBUG_BRIDGE_APPS_NOT_VERIFIED, 85




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Android Device - Compatibility not tested by Google	The profile of the Android device does not match the profile of any devices that have passed Google's testing Android compatibility testing. Vector: Device Tag: host.SafetyNetAttestation.ctsProfileMatch=false MITRE Tactics: Initial Access , Impact	Risk	Low	Yes	---	---	Yes (4.4)	Yes (4.4)	ANDROID_COMPATIBILITY_TESTING,70
Android Device - Possible Tampering	The Android device may have been tampered with. Vector: Device Tag: host.SafetyNetAttestation.basicintegrity=false MITRE Tactics: Execution , Persistence , Privilege Escalation , Impact	Threat	Critical	Yes	---	Yes	Yes (4.4)	Yes (4.4)	ANDROID_BASIC_INTEGRITY, 71
App Debug Enabled	An app with debug enabled can pose a risk and allow an attacker to control and manipulate the underlying app functions. Vector: Device Tag: host.app_attached_to_debugger MITRE Tactics: n/a	Risk	Elevated	Yes	---	---	Yes (4.16)	Yes (4.16)	DEBUG_ENABLED_APP, 103
App Running on Emulator	An app running on an emulator can pose a risk and allow an attacker to control and manipulate the underlying operating environment. Vector: Device Tag: host.app_running_on_emulator MITRE Tactics: n/a	Threat	Critical	Yes	---	---	---	Yes (4.16)	DEVICE_EMULATOR, 104




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
App Tampering	Existing app libraries may have been modified, or a foreign library may have been injected into the app. Vector: Device Tag: host.app_tampering MITRE Tactics: Execution , Persistence , Privilege Escalation , Defense Evasion	Threat	Critical	Yes	Yes	Yes	Yes (4.4)	Yes (4.4)	APP_TAMPERING,75
ARP Scan	A reconnaissance scan using the ARP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable for a network attack such as MITM. Vector: Network Tag: network.scan.arp MITRE Tactics: Network Effects , Discovery , Collection	Risk	Low	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	ARP_SCAN,3




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
BlueBorne Vulnerability	<p>zIPS has detected this device is vulnerable to BlueBorne, an attack leveraging Bluetooth connections to penetrate and take control of targeted devices. To avoid any sort of risk from BlueBorne, it is highly recommended that the user turns off Bluetooth permanently until an update is available from your device manufacturer or wireless carrier. For those users that still require the use of Bluetooth, it is recommended that Bluetooth is turned off until it is needed and only in a trusted and secure area.</p> <p>Vector: Device Tag:host.blueborne_vulnerability MITRE Tactics: Initial Access, Remote Service Effects</p>	Risk	Critical	Yes	--- (Yes for OS<= 9.3.5)	Yes	Yes	Yes [h]	BLUEBORNE_VULNERABLE, 69
Captive Portal	<p>The device is connected to a captive portal.</p> <p>Vector: Network Tag:network.captive_portal MITRE Tactics: Network Effects, Initial Access</p>	Risk	Low	Yes	Yes [a]	Yes	Yes	Yes [a]	CAPTIVE_PORTAL, 67




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Compromised Network	A pattern of threats that indicate the device is connected to a compromised network. Sensitive data on the device may be intercepted and could be monitored and modified by an unauthorized party. Type is composite. [f] Vector: Network Tag: pattern.compromised_network MITRE Tactics: Initial Access , Collection , Exfiltration , Network Effects	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	COMPROMISED_NETWORK, 125
Daemon Anomaly	Daemon Anomaly indicates abnormal system process activities which could indicate that the device has been exploited. Vector: Device Tag: host.daemon_anomaly MITRE Tactics: Execution , Persistence , Privilege Escalation	Risk	Normal	Yes (OS<=6 & Knox >= 3.4+)	---	---	Yes	Yes	DAEMON_ANOMALY, 43
Danger Zone Connected	The device has connected to a Wifi network where malicious events have been observed. Vector: Network Tag: network.danger_zone_connected MITRE Tactics: Initial Access , Network Effects	Threat	Elevated	Yes	Yes	Yes	Yes (4.4)	Yes (4.7) [h]	DANGERZONE_CONNECTED, 79




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Danger Zone Nearby	The device is near a Wi-Fi network where malicious attacks have been observed. Vector: Network Tag: network.danger_zone_nearby MITRE Tactics: Initial Access , Network Effects	Risk	Low	Yes	Yes [a]	Yes	Yes (4.4)	Yes (4.7) [h]	DANGERZONE_NEARBY, 80
Developer Options	Developer Options is an advanced configuration option intended for development purposes only. When enabled, the user has the option to change advanced settings, compromising the integrity of the device settings. Vector: Device Tag: host.developer_options MITRE Tactics: Impact	Risk	Elevated	Yes	---	Yes	Yes	Yes	DEVELOPER_OPTIONS_ON, 47
Device compromised via iOS Malicious Profile	The device was compromised by a sophisticated kill chain attack that started with a malicious iOS profile and ended leaving the device compromised. Type is composite. [f] Vector: Malware Tag: pattern.device_compromised_via_ios_malicious_profile MITRE Tactics: Initial Access , Execution , Persistence , Privilege Escalation , Credential Access , Collection , Exfiltration , Impact	Threat	Critical	---	Yes	---	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_IOS_MALICIOUS_PROFILE, 124




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Device Compromised via Malicious App	The device was compromised by a sophisticated kill chain attack that started with a malicious app and ended leaving the device compromised. Type is composite. [f] Vector: Device Tag: pattern.device_compromised_via_malicious_app MITRE Tactics: Initial Access , Execution , Persistence , Privilege Escalation , Credential Access , Collection , Exfiltration , Impact	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_MALICIOUS_APP, 122
Device Compromised via Network-Based Effects	The device was compromised by a sophisticated kill chain attack that started at the network and ended leaving the device compromised. Type is composite. [f] Vector: Network Tag: pattern.device_compromised_via_network_based_attacks MITRE Tactics: Initial Access , Execution , Persistence , Privilege Escalation , Credential Access , Collection , Exfiltration , Impact , Network Effects	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_NETWORK_BASED_ATTACKS, 121




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Device Compromised via Phishing Attack	The device was compromised by a sophisticated kill chain attack that started with a phishing threat and ended leaving the device compromised. Type is composite. [f] Vector: Network Tag: pattern.device_compromised_via_phishing_attack MITRE Tactics: Initial Access , Execution , Persistence , Privilege Escalation , Credential Access , Impact , Network Effects	Threat	Critical	Yes	Yes	Yes	Yes (4.17)	Yes (4.17)	DEVICE_COMPROMISED_VIA_PHISHING_ATTACK, 123
Device Encryption	Device Encryption notifies an administrator when a device is not set up to use encryption to protect device content. Vector: Device Tag: host.encryption MITRE Tactics: Impact	Risk	Elevated	Yes	---	n/a	Yes	Yes	ENCRYPTION_NOT_ENABLED, 49
Device Jailbroken/Rooted	Jailbreaking and rooting are the processes of gaining unauthorized access or elevated privileges on a system. Jailbreaking and rooting can potentially open security holes that may have not been readily apparent, or undermine the device's built-in security measures. Vector: Device Tag: host.jailbroken MITRE Tactics: Execution , Persistence , Privilege Escalation	Threat	Critical	Yes	Yes	Yes	Yes	Yes	DEVICE_ROOTED, 39




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Device Pending Activation	Device activation for zIPS not complete. A device that has synchronized through MDM but has not yet started zIPS. At the time at which the device would have previously become dormant, it now becomes Pending Activation because zIPS has never logged in. Notification email: [c] Vector: Device Tag: host.device_pending_activation MITRE Tactics: n/a	Risk	Low	Yes	Yes	Yes	Yes	Yes	INCOMPLETE, 200
Device Pin	Device Pin notifies the administrator when a device is not set up to use a PIN code or password to control access to the device. Vector: Device Tag: host.pin MITRE Tactics: Impact	Risk	Elevated	Yes	Yes	---	Yes	Yes	PASSCODE_NOT_ENABLED, 50
DNS Change	DNS configuration changes on the mobile device. If the DNS change happened in your own network to an unknown DNS server - it is likely to be a MITM attempt. Vector: Device Tag: host.config.dns MITRE Tactics: Initial Access , Network Effects	Risk	Low	Yes	---	Yes	Yes	Yes	DNS_CHANGE, 17



Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Elevation of Privileges (EOP)	A malicious process that results in the elevation of privileges on the mobile device, which allows the attacker to take full control of the device. Vector: Device Tag: host.process.eop MITRE Tactics: Execution , Persistence , Privilege Escalation	Threat	Critical	Yes (OS<=6 & Knox >= 3.4+)	Yes	---	Yes	Yes	RUNNING_AS_ROOT, 12
File System Changed	A normal file system change. Modification(s) made to files in the file system that sometimes lead to a malicious event. Vector: Device Tag: host.process.filesystemchange MITRE Tactics: Persistence , Impact	Threat	Critical	Yes	Yes	Yes	Yes	Yes	FILES_SYSTEM_CHANGED, 23
Gateway Change	Gateway configuration changes on the mobile device that can be indicative of sending traffic to a non-intended destination. Vector: Network Tag: host.config.gateway MITRE Tactics: Initial Access , Network Effects	Risk	Low	Yes	---	---	Yes	Yes	GATEWAY_CHANGE, 16
Google Play Protect Disabled	Google Play Protect has been disabled on this device. Google Play Protect helps protect the device from malicious apps and should be re-enabled. Vector: Device Tag: host.config.google_play_protect_disabled MITRE Tactics: Initial Access , Impact	Risk	Elevated	Yes	---	Yes	Yes (4.5)	Yes (4.5)	GOOGLE_PLAY_PROTECT_DISABLED, 84




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Inactive Device	Occurs whenever the device does not communicate with the server for a certain amount of time. This is typically a time as defined by the dormancy configuration. Notification email: [c] Vector: Device Tag: app.dormant MITRE Tactics: n/a	Risk	Low	Yes	Yes	Yes	Yes	---	DORMANT, 100
Internal Network Access	Detected an app connecting to private, internal servers. It is uncommon for public applications to connect to internal servers. Public applications connecting to internal servers are considered suspicious behavior and should be investigated immediately for the possible threat of malware installed on the device and the risk of data leakage. Vector: Network Tag: network.internal_network_access MITRE Tactics: Discovery , Lateral Movement , Collection	Risk	Elevated	Yes (OS<=9 & Knox >= 3.4+)	---	---	Yes	Yes	INTERNAL_NETWORK_ACCESS, 48




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
IP Scan	A reconnaissance scan using the IP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable to a network attack such as MITM. This is an early indication of a network reconnaissance probe. Vector: Network Tag: network.scan.ip MITRE Tactics: Initial Access , Discovery , Collection , Network Effects	Risk	Low	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	IP_SCAN, 2
MITM	Man-in-the-Middle attack where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device. Vector: Device Tag: network.mitm MITRE Tactics: Collection , Exfiltration , Network Effects	Threat	Critical	Yes	Yes	Yes	Yes	Yes	TRACEROUTE_MITM, 68
MITM - ARP	Man-in-the-Middle attack using ARP table poisoning where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device. Vector: Network Tag: network.mitm.arp MITRE Tactics: Collection , Exfiltration , Network Effects	Threat	Critical	Yes (OS<=9)	Yes (OS<=10) [e]	---	Yes	Yes	ARP_MITM, 4




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
MITM - Fake SSL Certificate	Man-in-the-Middle attack using fake certificates where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device. Vector: Network Tag: network.mitm.ssl_certificate MITRE Tactics: Collection , Exfiltration , Network Effects	Threat	Critical	Yes	Yes	Yes	Yes	Yes	SSL_MITM, 35
MITM - ICMP Redirect	Man-in-the-Middle attack using ICMP protocol where a malicious attacker can hijack traffic and steal credentials or deliver malware to the device. Vector: Network Tag: network.mitm.icmp MITRE Tactics: Collection , Exfiltration , Network Effects	Threat	Critical	Yes (OS<=9)	---	---	Yes	Yes	ICMP_REDIRECT_MITM, 11
MITM - SSL Strip	Man-in-the-Middle attack using SSL stripping that allows a malicious attacker to change HTTPS traffic to HTTP so they can hijack traffic and steal credentials or deliver malware to the device. Vector: Network Tag: network.mitm.ssl_strip MITRE Tactics: Collection , Exfiltration , Network Effects	Threat	Critical	Yes	Yes	Yes	Yes	Yes	SSL_STRIP, 14




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Network Handoff	Network handoff allows a device to alter routing on a network, potentially allowing for a man-in-the-middle attack. Vector: Network Tag: network.arp.handoff MITRE Tactics: Initial Access , Network Effects , Exfiltration	Risk [d]	Low	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	NETWORK_HANDOFF, 36
Out of Compliance App	This threat is sent to a device when apps marked 'Out of Compliance' are found on the device. Vector: Device Tag: host.app_out_of_compliance MITRE Tactics: Exfiltration , Collection , Impact	Risk	Elevated	Yes	Yes	Yes	Yes (4.9)	Yes (4.9) [h]	OUT_OF_COMPLIANCE_APP, 93
Over-The-Air (OTA) Updates Disabled	Over-the-air (OTA) updates have been disabled on this device. OTA updates help keep a device's software up to date and more secure. Vector: Device Tag: host.ota_updates_disabled MITRE Tactics: Impact	Risk	Elevated	Yes	---	Yes	Yes (4.8)	Yes (4.8)	OVER_THE_AIR_UPDATES_DISABLED, 86
Phishing Protection - Link Tapped	A potentially malicious URL was tapped on the device. Vector: Device Tag: host.site-insight.link-tapped MITRE Tactics: Initial Access , Credential Access , Network Effects	Risk	Low	Yes	Yes	Yes	Yes	Yes [h]	MALICIOUS_WEBSITE, 9



Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Phishing Protection - Link Visited	A potentially malicious URL was tapped on the device. The user was warned of the potential danger of visiting the linked site and chose to continue on to the site after the warning. Vector: Device Tag: host.site-insight.link-visited MITRE Tactics: Initial Access , Credential Access , Network Effects , Execution , Privilege Escalation	Threat	Elevated	Yes	Yes	Yes	Yes	Yes [h]	MALICIOUS_WEBSITE_OPENED, 72
Proxy Change	Proxy configuration changes on the mobile device that can be indicative of sending traffic to a non-intended destination. Vector: Network Tag: host.config.proxy MITRE Tactics: Initial Access , Network Effects , Exfiltration	Risk	Low	Yes	---	---	Yes	Yes	PROXY_CHANGE, 15
Rogue Access Point	Rogue Access Point exploits a device vulnerability to connect to a previously known Wi-Fi network by masking preferred/known networks. Vector: Network Tag: network.mitm.rogue_ap MITRE Tactics: Network Effects , Initial Access , Credential Access	Threat	Critical	Yes [g]	Yes	Yes	Yes	Yes	ROGUE_ACCESS_POINT, 38
Rogue Access Point: Nearby	The device is in close proximity to a malicious/rogue access point. Vector: Network Tag: network.mitm.rogue_ap_nearby MITRE Tactics: Initial Access , Network Effects	Risk	Low	Yes [g]	---	Yes	Yes	Yes	ROGUE_ACCESS_POINT_NEARBY, 65




Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
SELinux Disabled	Security-enhanced Linux (SELinux) is a security feature in the operating system that helps maintain the integrity of the operating system. If SELinux has been disabled, the integrity of the operating system may be compromised and should be investigated immediately. Vector: Device Tag: host.selinux.disabled MITRE Tactics: Impact	Threat	Critical	Yes	---	---	Yes	Yes	SELINUX_DISABLED, 61
Sideloaded App(s)	Sideloaded apps are installed independently of an official app store and can present a security risk. Vector: Malware Tag: host.sideloaded_app MITRE Tactics: Initial Access , Collection , Exfiltration , Persistence	Risk	Elevated	Yes	Yes	Yes	Yes (4.7)	Yes (4.7)	SIDLOADED_APP, 76
SSL/TLS Downgrade	SSL/TLS downgrades force apps to use old encryption protocols. These protocols may be vulnerable to attacks that allow third parties to view encrypted information. Vector: Network Tag: network.ssl_tls_downgrade MITRE Tactics: Impact , Network Effects	Threat	Elevated	Yes	Yes	---	Yes (4.4)	Yes (4.4)	TLS_DOWNGRADE, 77
Stagefright Vulnerability	Stagefright vulnerability indicates the device is on an OS patch version susceptible to compromise. Vector: Device Tag: host.mediaserver.sf_vulnerability MITRE Tactics: Impact	Risk	Critical	Yes	---	Yes	Yes	Yes	STAGEFRIGHT_VULNERABLE, 40

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Suspicious Android App	A known malicious app that attempts to take control of the device in some manner (for instance, elevate privileges or spyware). Vector: Malware Tag: host.app.malicious MITRE Tactics: Initial Access , Persistence , Exfiltration , Impact , Credential Access , Execution , Collection	Threat	Critical	Yes	---	Yes	Yes	Yes	APK_SUSPECTED, 13
Suspicious iOS App	A known malicious app that attempts to take control of the device in some manner (for instance, elevate privileges or spyware). Vector: Malware Tag: host.ipa.malicious MITRE Tactics: Initial Access , Persistence , Exfiltration , Impact , Credential Access , Execution , Collection	Threat	Critical	---	Yes [b]	n/a	Yes	Yes [h]	SUSPICIOUS_IPA, 42
Suspicious Profile	A suspicious profile is a new profile introduced to the environment and is not explicitly trusted or untrusted. It is recommended that the Administrator review the Profile and mark the profile as trusted or untrusted. Vector: Device Tag: host.profile.suspicious MITRE Tactics: Initial Access , Persistence , Exfiltration , Impact , Credential Access , Execution , Collection	Risk	Elevated	---	Yes [b]	n/a	Yes	---	SUSPICIOUS_PROFILE, 45

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
System Tampering	System Tampering is a process of removing security limitations put in by the device manufacturer and indicates that the device is fully compromised and can no longer be trusted. Vector: Device Tag: host.systemconfig.system_tampering MITRE Tactics: Execution , Privilege Escalation , Impact	Threat	Critical	Yes	Yes	Yes	Yes	Yes	SYSTEM_TAMPERING, 37
TCP Scan	A reconnaissance scan using the TCP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable to a network attack such as MITM. Vector: Network Tag: network.scan.tcp MITRE Tactics: Initial Access , Discovery , Collection , Network Effects	Risk	Elevated	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	TCP_SCAN, 0
UDP Scan	A reconnaissance scan using the UDP protocol that is oftentimes an indicator of a malicious attacker searching for a device vulnerable to a network attack such as MITM. Vector: Network Tag: network.scan.udp MITRE Tactics: Initial Access , Discovery , Collection , Network Effects	Risk	Low	Yes (OS<=9)	Yes (OS<=9)	---	Yes	Yes	UDP_SCAN, 1

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Unknown Sources Enabled	Allowing you to download an app that is not on the Google Play store. Vector: Device Tag: host.config.unknown_sources MITRE Tactics: Impact , Initial Access	Risk	Critical	Yes (OS<=7)	---	Yes	Yes	Yes	UNKNOWN_SOURCES_ON, 25
Unsecured Wi-Fi Network	An open unsecured Wifi network has been connected. Vector: Network Tag: network.unsecured.wifi MITRE Tactics: Initial Access , Network Effects , Exfiltration , Collection	Risk	Elevated	Yes	Yes[a]	---	Yes	Yes[a]	UNSECURED_WIFI_NETWORK, 66
Untrusted Profile	An untrusted profile is a profile installed on one or more devices and is deemed unsafe to have installed on your devices. An untrusted profile installed on devices could be used to control devices remotely, monitor and manipulate user activities, and/or hijack a user's traffic. Vector: Device Tag: host.profile.untrusted MITRE Tactics: Initial Access , Persistence , Exfiltration , Impact , Credential Access , Execution , Collection	Threat	Critical	---	Yes [b]	n/a	Yes	Yes [h]	UNTRUSTED_PROFILE, 24

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
USB Debugging Mode	<p>USB Debugging is an advanced configuration option intended for development purposes only. By enabling USB Debugging, your device can accept commands from a computer when plugged into a USB connection.</p> <p>Vector: Device Tag:host.usb.debugging MITRE Tactics: Impact, Initial Access</p>	Risk	Elevated	Yes	---	Yes	Yes	Yes	USB_DEBUGGING_ON, 44
Vulnerable Android Version	<p>zIPS has detected that the Android version installed on your device is not up-to-date. The outdated operating system exposes the device to known vulnerabilities and the threat of being exploited by malicious actors. It is advised to update your operating system immediately.</p> <p>Vector: Device Tag:host.vulnerable.android MITRE Tactics: Impact</p>	Risk	Elevated	Yes	---	Yes	Yes	Yes [h]	ANDROID_NOT_UPDATED, 51
Vulnerable iOS Version	<p>zIPS has detected that the iOS version installed on your device is not up-to-date. The outdated operating system exposes the device to known vulnerabilities and the threat of being exploited by malicious actors. It is advised to update your operating system immediately.</p> <p>Vector: Device Tag:host.vulnerable.ios MITRE Tactics: Impact</p>	Risk	Elevated	---	Yes	n/a	Yes	Yes [h]	IOS_NOT_UPDATED, 52

Threat Name	Threat Description	Risk or Threat	Severity Default				zIPS	zDefend SDK	Threat Identifiers
Vulnerable, Non-Upgradeable Android Version	zIPS detected a device running a vulnerable Android version. However, the device is not eligible for an operating system upgrade at this time. Vector: Network Tag: host.vulnerable.android.non-upgradeable MITRE Tactics: Impact	Risk	Low	Yes	---	Yes	Yes (4.4)	Yes (4.4) [h]	VULNERABLE_NON_UPGRADEABLE_ANDROID_VERSION, 89
Vulnerable, Non-Upgradeable iOS Version	zIPS detected a device running a vulnerable iOS version. However, the device is not eligible for an operating system upgrade at this time. Vector: Network Tag: host.vulnerable.ios.non-upgradeable MITRE Tactics: Impact	Risk	Low	---	Yes	n/a	Yes (4.4)	Yes (4.4) [h]	VULNERABLE_NON_UPGRADEABLE_IOS_VERSION, 88
zIPS Is Not Activated on Both Work and Personal Profiles – Android Enterprise	zIPS is not activated on both the personal and work profiles on this device. Install and activate the application in both locations to ensure full device protection. Vector: Device Tag: host.afw_both_profiles_not_activated MITRE Tactics: n/a	Risk	Elevated	Yes	---	n/a	Yes (4.4)	---	ZIPS_NOT_RUNNING_ON_CONTAINER, 78

Threat List Legend

[a] = Indicates that for iOS support, Hotspot Helper is required.

[b] = Indicates that for iOS threat support, an MDM server to sync with the zConsole is required.

[c] = Indicates that the server detects the threat and sends a notification (email) without a device alert display within the application.

[d] = Indicates the value is really a mitigation of a previous MITM-ARP threat.

[e] = MITM – ARP is supported on iOS 10 only. For iOS 11 and above, the MITM attacks are detected under the threat name MITM.

[f] = Indicates that the threat is a composite threat. See the “Zimperium zConsole Configuration Guide” for definitions of composite and singular threats.

[g] = Indicates that a particular type of Rogue Access Point threat called KARMA is only supported by Android OS 9 and earlier.

[h] = Indicates that the zDefend SDK can return this threat, but the threat only applies when interfacing with the v4 zConsole.