Zimperium Mobile Threat Defense (zIPS) Comparison Test for Android

A test commissioned by Zimperium and performed by AV-TEST GmbH
Date of the report: November 10th, 2022, last update: December 13th, 2022

Executive Summary

In October/November 2022, AV-Test performed a comparative review of Zimperium Mobile Threat Defense solution (zIPS) to determine the prevalent and real-time prevention detection of the product run in online and offline mode. The offline test mode should demonstrate the protective effect of Mobile Threat Defense for customers at any time, regardless of the state of connectivity. Alongside the normal online Mobile Threat Defense device, AV-TEST has run all tests in parallel with a device with Mobile Threat Defense installed where Wi-Fi and cellular network were turned off.

The prevalent malware test corpus consisted of 2984, and the real-time test corpus of 3292 malicious apps.
For all the following tests, a clean Android 11 was used on identical Motorola moto g30 devices. At first, AV-TEST started with an on-demand test, which involved scanning all samples on the SD card of a device. The Zimperium solution was installed on the device, and the samples were pushed to the SD card and a scan was performed. The result of the scan was captured, and the detected samples were deleted. The not detected samples were pulled from the device and became the basis for the followed up prevalent on-access test.
The prevalent on-access test checks the Zimperium MTDs capability of detecting apps upon installation on device. On the device, the Zimperium solution was installed, as well as AV-TEST's two Android test apps. Those two apps are used to determine the detections of the product and the connectivity state of the device. Each malware sample that was not detected during the on-demand scan was installed on the device, and any detection by the Zimperium MTD solution was recognized by the monitoring app. After a period of time, the malware sample was uninstalled from the device, and the next sample was processed.
The real-time test follows the same workflow as described for the on-access test of the prevalent test. In contrast to the prevalent test, only newly discovered malware samples are used. To achieve the best comparability of the results in real-time testing, this test is performed simultaneously.

A false positive test is a counterpart for malware detection tests. Clean samples are used to check whether a product detects them as malicious and causes disruption in the user experience.
For this test, the same workflow as described for the on-access test of the prevalent test was used.

Zimperium delivered an outstanding performance for both the online and the offline modes when it comes to prevalent malware detection. In real-time testing, the offline product could almost compete with the excellent result of the online product. In regard to the false positive testing, both the online and offline products did a good job by only having one false detection.

Overview

With the increasing number of threats being released and spreading through the Internet these days, the danger of getting infected is also increasing. A few years back, there were new malware apps released every few days. This has grown to several thousand new threats per day. As of November 2022, AV-TEST has already recognized over 1 million new Android malware samples for the year of the report.
Infections with Android malware can cause financial losses, private data losses, or even damaged hardware. A Banking-Trojan can steal credit data, while a Backdoor might open unwanted access to the device, and a Ransomware-App can prevent the normal usage of the device.
The task of an anti-malware product is to protect a user against such threats at any time of usage.

Methodology and Scoring

Products Tested

AV-TEST used the latest releases available at the time of the test of the following product:

(1) Zimperium Mobile IPS (zIPS) 4.22.5

In the following pages, we will refer to zIPS as in online operation mode while zIPS Offline is used for operation offline mode.

Platform

All tests have been performed on identical Motorola moto g30 devices with the following specifications:

- Model XT2129-2
- Display 16.5 cm (6.5")
- CPU 2 GHz Qualcomm Snapdragon 662 Octa-Core-Processor
- RAM 4 GB
- Memory 128 GB, MicroSD-Slot, Dual-Sim
- Connectivity LTE (4G), Wi-Fi 5 (802.11ac), Bluetooth, NFC, GPS

Operating system Android 11, build number RRCS31.Q1-3-68-4

General Approach

1. **No rooted devices are used for testing.**
2. **Only clean restored devices are used for each test.**
3. **Only physical devices are used for testing**.
4. **At any state of the test the online connectivity is ensured for the online mode device.**
5. **Android samples are only installed and not launched.**

Prevalent Test

The prevalent test has been performed according to the methodology explained below.

The prevalent test consists of 2 parts, an on-demand scan, and on-access test.
The first part of the prevalent test is the on-demand scan.

On-Demand Scan

Test steps:

1. Samples are pushed to the SD card via the Android Debug Bridge
2. The on-demand scan of the product is started.
3. Upon finish of the on-demand scan, the results presented by the product are documented (e.g., by creating screenshots or storing report files)
4. Detected samples are deleted by the product
5. The remaining samples are pulled from the SD card via the Android Debug Bridge

The pulled (not detected) samples are the basis for the second part of the prevalent test: the on-access test.

On-Access Test

Device preparation:

- Installation of AV-TEST's two Android test apps alongside the Zimperium MTD solution to recognize the detections of the product and the connectivity state of the device.

Test steps:

1. Internet connectivity check on the device
2. Installation of the sample via the Android Debug Bridge
3. Notifications from the anti-virus app are recognized and documented by AV-TEST's app (e.g., by creating screenshots or storing report files)
4. For documentation, a screenshot of the device screen is taken
5. Uninstallation of the sample via the Android Debug Bridge
6. Home-Button is pressed

Steps 1 to 6 are repeated for each sample.

Real-Time Test

The real-time test has been performed according to the methodology explained below.

Device preparation:

- Installation of AV-TEST's two Android test apps alongside the Zimperium MTD to recognize the detections of the product and the connectivity state of the device.

Test steps:

1. Internet connectivity check on the device
2. Installation of the sample via the Android Debug Bridge
3. Notifications from the anti-virus app are recognized and documented by AV-TEST's app (e.g., by creating screenshots or storing report files)
4. For documentation, a screenshot of the device screen is taken
5. Uninstallation of the sample via the Android Debug Bridge
6. Home-Button is pressed

Steps 1 to 6 are repeated for each sample. After 100 samples, the devices are rebooted.

False-Positive Test

The false-positive test has been performed according to the methodology explained below.

Device preparation:

- Installation of AV-TEST's two Android test apps alongside the Zimperium MTD to recognize the detections of the product and the connectivity state of the device.

Test steps:

1. Internet connectivity check on the device
2. Installation of the sample via the Android Debug Bridge
3. Notifications from the anti-virus app are recognized and documented by AV-TEST's app (e.g., by creating screenshots or storing report files)
4. For documentation, a screenshot of the device screen is taken
5. Uninstallation of the sample via the Android Debug Bridge
6. Home-Button is pressed

Steps 1 to 6 are repeated for each sample.

Performance Test

AV-Test emulates the average daily usage of a device.
One test cycle consists of:

- Installing 33 apps
- Browsing 20 websites
- Watching YouTube
- Reading PDF documents
- Idle with screen turned off 60 Minutes

The test cycle is repeated 7 times.

Malware Samples

The test set consisted of 2984 prevalent samples and 3292 real-time samples that could harm an Android device. The prevalent malware set contained the most common Android malware samples, which were not older than 4 weeks before the test. Real-time malware samples consisted of Android malware samples, which were first seen within the last 24 hours in AV-TEST's database and were tested on the day of their discovery.

False-Positive Samples

AV-TEST's false-positive test is divided into two parts; for the first part, apps from Google Play are used. Apps from third-party stores from around the world are the basis for the second part of the test. 1924 apps from Google Play and 1297 apps from third-party stores have been collected by AV-TEST for this Android test.

Test Results

Prevalent Test

The prevalent test shows how well the Zimperium MTDs can detect the most common threads from the past 4 weeks. The following figure shows the overall prevalent detection rate of Mobile IPS and Mobile IPS Offline.

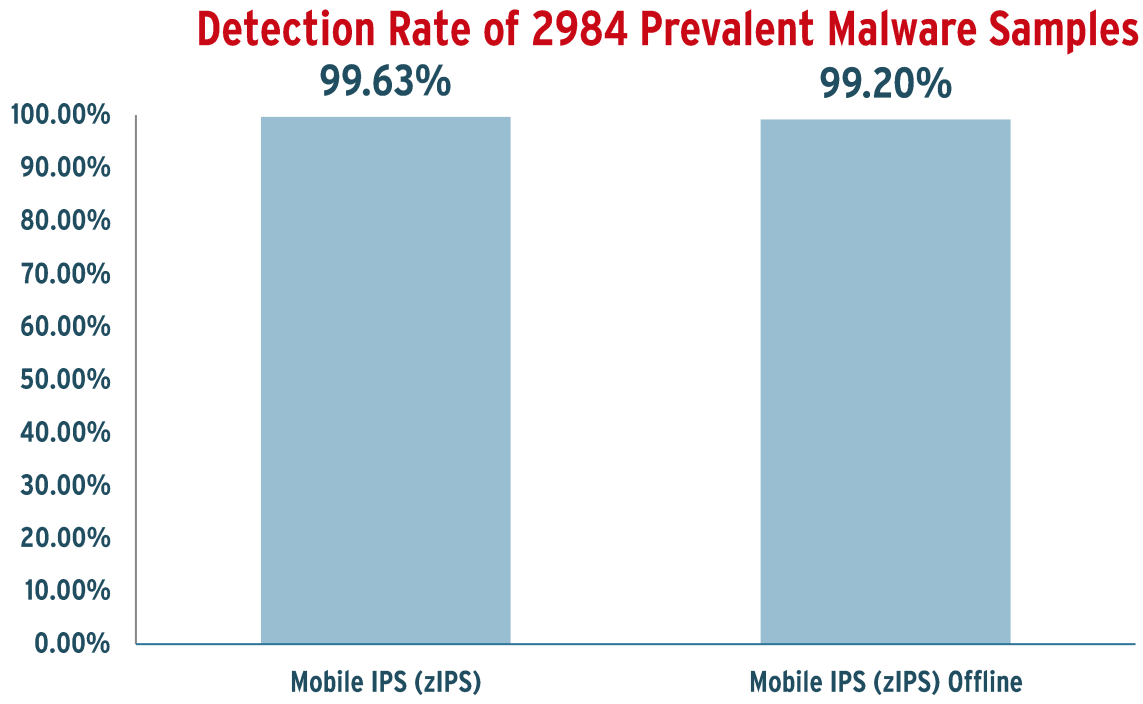

Figure 2: Prevalent Test

Zimperium delivered a great performance for both the online and the offline mode by detecting 99.63% and 99.20% of every malware sample of the 2984 malicious apps AV-TEST has tested. The detection rate is calculated by the samples detected during the on-demand test, where the SD card is scanned, and the on-access test, where the remaining samples of the on-demand test are installed on a device.

Real-Time Test

This test was performed simultaneously with both Mobile IPS and Mobile IPS Offline. The purpose of the test is to show how well the Zimperium MTD solution reacts to newly discovered threats. A new threat, in this case, is meant by new malware samples, which is first seen by AV-TEST within the last 24 hours prior to the test time. The following figure shows the overall real-time detection rate of Mobile IPS and Mobile IPS Offline.

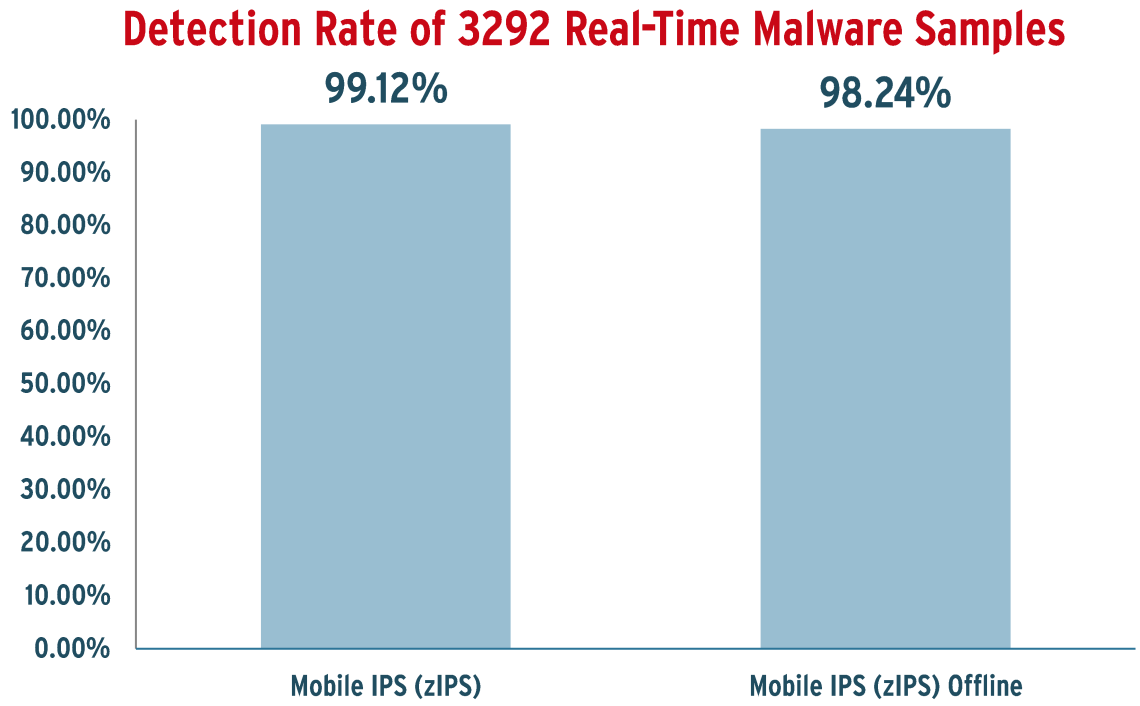

Figure 3: Real-Time Test

Zimperium Mobile IPS in online mode delivered a great performance in detecting 99.12% of the 3292 malicious apps used for the real-time test. The offline product could almost compete with the great result of the online product by detecting 98.24%. The most remarkable aspect that could be seen from Figure 3 is that Mobile IPS in offline mode is only missing the detection rate of Mobile IPS in online mode by less than one percent.

False-Positive Test

Mobile IPS and Mobile IPS Offline both delivered a great performance by not detecting any of the 1297 tested clean apps from the Play Store. While for 1297 apps from third-party stores both wrongly flagged the same clean app as harmful. In both modes, Zimperium did a good job when compared to the number of samples tested.

Performance Test

	Zimperium Mobile IPS (zIPS)	Zimperium Mobile IPS (zIPS) Offline
The app does not reduce the battery life *Median CPU usage < 20% in idle	0.03%	0.04%
The app does not slow down the device during normal usage *Median CPU usage < 10% for:		
Loading websites with Android browser	0.24%	0.25%
Watching videos with YouTube app	0.03%	0.04%
Reading PDF documents with Adobe Reader app	0.37%	0.38%
The app does not generate a lot of traffic *Median Traffic < 5000 Bytes in idle	142 Bytes	0 Bytes

Both Zimperium Mobile IPS in online and offline mode did not show any impact on the user experience. They did not reduce the battery life, did not slow down the device during normal usage, or did generate a lot of traffic.