



Q1 2017
Advanced Threat Defense
Certification Testing Report

Kaspersky Lab
Kaspersky Anti Targeted Attack Platform (KATA)
ICSA Labs Advanced Threat Defense Criteria v.1.0

April 5, 2017

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

ATD-KASPERSK-2017-0405-01

ICSA Labs Advanced Threat Defense – Report-at-a-Glance

Kaspersky Lab



Kaspersky Anti Targeted Attack Platform

www.kaspersky.com/enterprise-security/anti-targeted-attack-platform

Executive Summary

During 40 consecutive days of testing during the first quarter of 2017, ICSA Labs tested the detection capabilities of Kaspersky Anti Targeted Attack Platform (KATA) with a mix of over 900 test runs. The mix was primarily composed of new and little-known malicious threats – i.e., recently harvested threats not detected by traditional security products.

Periodically, ICSA Labs launched innocuous applications and activities to additionally test the KATA platform in terms of false positives. Throughout testing, ICSA Labs observed product logs to ensure not only that the KATA platform indicated the existence of a malicious threat but also that logged threats were distinguishable from other logged traffic and events.

The KATA platform passed, having met all criteria requirements. As seen in Figure 1 below, Kaspersky’s solution did remarkably well during this test cycle - detecting 99.53% of previously unknown threats while having zero false positives! Figures 2 and 3 below further highlight the solution’s detection effectiveness and false positives.

Test Length	40 days	Malicious Samples	428	Innocuous Apps	490
Test Runs	918	% Detected	99.53%	% False Positives	0.0%

Fig. 1 – High Detection Effectiveness & Few False Positives

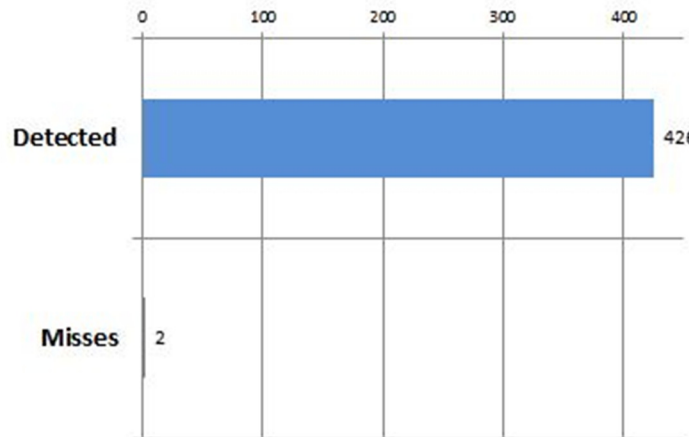


Fig. 2 – Detected 426 of 428 *New & Little-Known* Malicious Samples



Fig. 3 – No Alerts on Innocuous Applications

ICSA Labs
Advanced Threat Defense

Certified

Test Period: Q1 2017
Certified Since: 12 / 2016

Introduction

This is Kaspersky Lab's second consecutive ICSA Labs Advanced Threat Defense Certification testing report for Kaspersky Anti Targeted Attack Platform (KATA).

Standard ICSA Labs Advanced Threat Defense (ATD) testing is aimed at vendor solutions designed to detect new threats that other traditional security products miss. Thus the focus is on how effectively vendor ATD solutions detect these unknown and little-known threats while minimizing false positives.

The remainder of the report presents a more detailed look at how the Kaspersky Lab KATA advanced threat defense solution performed during this cycle of standard ICSA Labs ATD Certification testing. To better understand how to interpret the results, this report documents not just the testing results themselves but the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against Kaspersky Lab's KATA.

Test Cycle Information

This report reflects the results of one test cycle at ICSA Labs. Standard ATD and ATD-Email test cycles are performed by ICSA Labs each calendar quarter and typically range from three to five weeks in duration. To be eligible for certification, security vendor solutions must be tested for at least 3 weeks. Because testing is performed quarterly, ICSA Labs tests ATD solutions four times during a calendar year.

During each test cycle ICSA Labs subjects advanced threat defense solutions to hundreds of test runs. The test set is comprised of a mix of new threats, little-known threats and innocuous applications and activities – delivered and launched one after another continuously for the length of testing. Below in Figure 4 is information about the test cycle from which this findings report is based. Note that this test cycle extended beyond the usual 5 weeks:

Start Date	Jan. 17, 2017	Days of Continuous Testing	40
End Date	Feb. 25, 2017	Test Runs	918

Fig. 4 – This Test Cycle

ATD Solution Tested

During this testing cycle, ICSA Labs tested the Kaspersky Anti Targeted Attack Platform (KATA) from Kaspersky Lab.

- Kaspersky Anti Targeted Attack Platform – 1.0.1

Kaspersky Anti Targeted Attack Platform (KATA) uses multi-layered threat detection – including a granular assessment of activity that's occurring on the customer's corporate network and at endpoints – to help protect businesses and organizations against sophisticated threats and targeted attacks. KATA includes network sensors, web and email sensors, as well as optional endpoint sensors that together help to detect threats – not just at the entry points - but wherever they arise within the customer's IT infrastructure. KATA also includes Kaspersky's Targeted Attack Analyzer that assesses data from network and endpoint sensors – and rapidly generates threat detection verdicts for the security team. By combining sandbox-based analysis and Kaspersky's advanced machine learning technologies, Kaspersky Anti Targeted Attack Platform helps to deliver protection against a wider range of threats.

For more information about the Kaspersky Lab KATA, its component parts and related information please visit:

<https://www.kaspersky.com/enterprise-security/anti-targeted-attack-platform>

http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KATA_Feature_List.pdf

Detection Effectiveness

To meet the criteria requirements and attain (or retain) certification through ICSA Labs testing, advanced threat defense solutions must be at least 75% effective at detecting new malicious threats. As shown in Figure 5 the Kaspersky Lab KATA platform detected 99.53% of the threats it encountered during testing, considerably better than the percentage required for certification.

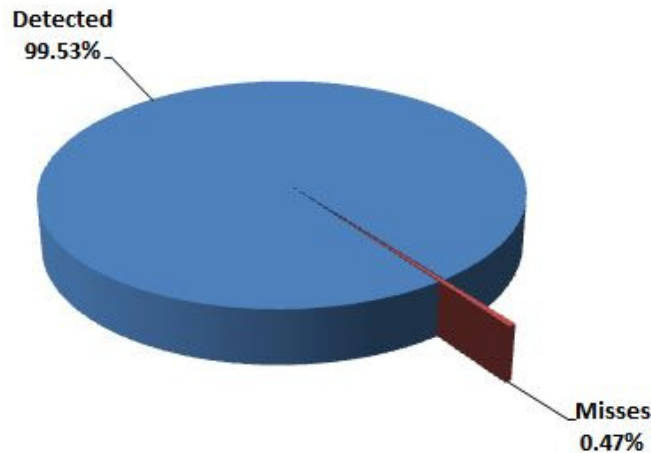


Fig. 5 – Detection Effectiveness of Kaspersky’s KATA

A second plot depicting the detection effectiveness of KATA appears in Figure 6. For Kaspersky Labs’ solution the chart sheds light on whether or not the KATA did better or worse – the newer the malicious sample. The Kaspersky KATA platform detected 100% of malicious threats that were one hour old or less, and also 100% of threats that were just 2 hours old. Overall the Kaspersky KATA platform did a very good job detecting new and little-known malicious threats regardless of their age.

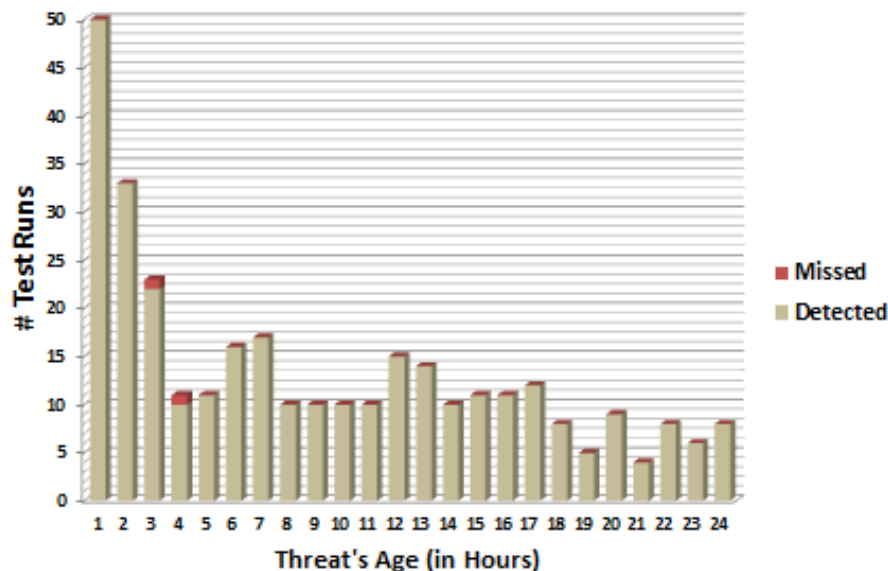


Fig. 6 – Detection Effectiveness by Age of Threat (Threats < 24 Hours Old)

A final effectiveness-related plot to consider for Kaspersky Labs' advanced threat defense solution KATA during this test cycle is Figure 7 below. Plotted below is each of the 40 days during the test cycle along with how effective the KATA platform was on each of those days. For an impressive thirty-nine of the forty days during the test cycle, the Kaspersky KATA platform was 100% effective against new and little-known threats.

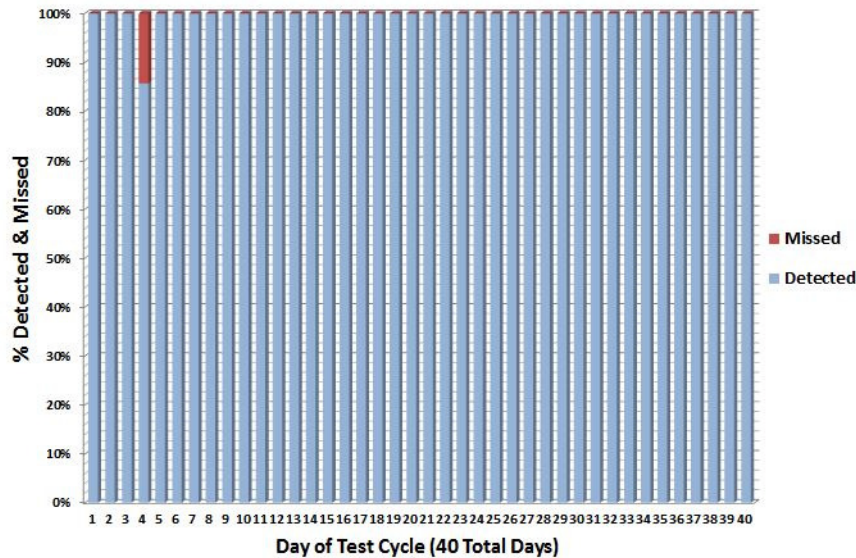


Fig. 7 – Detected & Missed Threats by Day of Test Cycle

Threat Vectors

In testing, ICSA Labs delivers new and little-known malicious threats to security vendor solutions using many of the top threat vectors that have led to enterprise cybersecurity incidents and breaches as reported in the latest [Verizon Data Breach Investigation Report \(DBIR\)](#).

DBIR data indicates that malware has been a key factor in thousands of security events where an information asset had its integrity, confidentiality, and/or availability compromised. Figure 9 on the following page depicts the threat vectors involved in these malware-related security incidents throughout the over ten year history of Verizon's DBIR. Figure 8 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2015 alone (2016 DBIR).

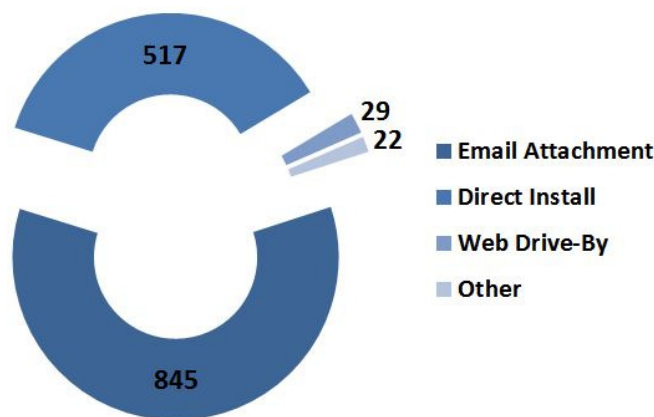


Fig. 8 – Top Threat Vectors Leading to Breaches in 2015 (2016 DBIR)

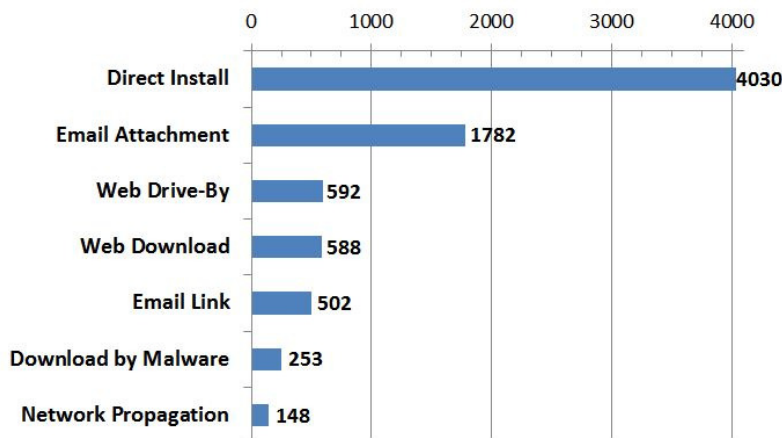


Fig. 9 – Malware-Related Threat Vectors Involved in Incidents (DBIR All-Time)

Standard ICSA Labs ATD testing includes the threat vector that is by far the most prevalent over time, “Direct Install”. In addition, standard ATD testing includes the threat vectors labeled “Web Download”, “Web Drive-By”, and “Download by Malware”. In the separate but related, ICSA Labs ATD-Email testing, ICSA Labs delivers new and little-known malware in URLs and attachments, corresponding to DBIR threat vectors “Email Link” and “Email Attachment”, the latter being the single most common threat vector leading to enterprise breaches according to the 2016 DBIR (refer to Figure 8 above).

Source of Samples

A number of sample sources feed ICSA Labs’ standard ATD and ATD-Email testing.

One source is the spam ICSA Labs collects. The labs’ spam honeypots receive approximately 250,000-300,000 spam email messages/day. For ICSA Labs ATD testing, the team harvests attachments in that spam, making use of the ones that are malicious.

Samples may also come from malicious URLs. Some of these come from the spam mentioned above. From feeds like this ICSA Labs filters and checks the URLs to see if there is a malicious file on the other end of that URL -- either as a direct file link or a series of steps (e.g. a drive-by attack with a multi-stage download process) leading to it. If so, ICSA Labs collects the sample for potential use in testing.

ICSA Labs additionally uses other tools and techniques to create unique malicious files as an attacker or penetration tester might do. In some cases these are trojanized versions of clean executables. In other cases they may be original executables that are malicious.

Still another source of samples is the samples themselves. Any dropped files resulting from running another malicious sample are also evaluated and potentially used in testing.

Finally – and importantly to test for false positives – ICSA Labs also launches legitimate executables. Running innocuous applications helps ensure that vendor solutions aren’t just identifying everything as malicious.

Ransomware Less Hot This Test Cycle

While Ransomware levels were off the charts throughout most of 2016, they were down significantly in the Q1 2017 test cycle. Figure 10 below indicates that there were just 133 messages per day on average with Ransomware archives attached. Thus, the average number of spam emails with ransomware received during the Q1 2017 ATD daily test cycle was over 68,000 fewer than the daily average the previous quarter.

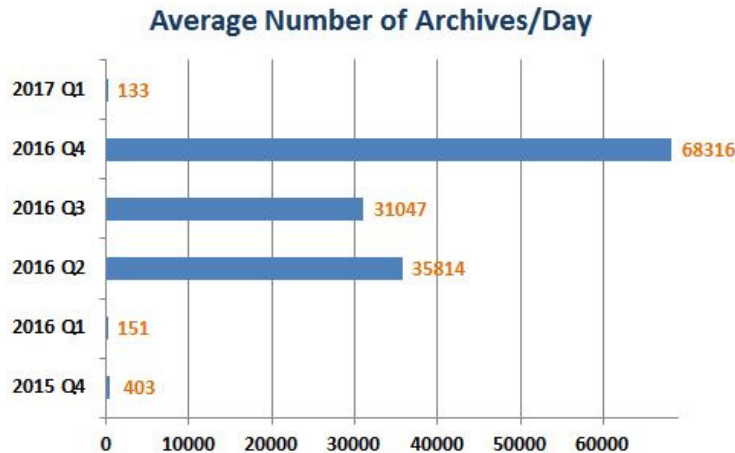


Fig. 10 – Ransomware Per Day Averages During Recent ATD Test Cycles

Regarding the Samples from This Test Cycle

Samples harvested for use in ATD testing are often unmodified and used as is. That is the case if ICSA Labs determines that the sample is new enough and/or not being detected by traditional security products. In many cases malicious samples require modification before they can avoid detection by traditional security products.

Of the 428 malicious samples, Figure 11 shows that there were many more original samples used and far fewer samples that required some kind of modification before use in testing. As there were many more unmodified samples, Figure 12 reveals the source of the 335 malicious samples used in testing that were both unmodified and non-dropped (i.e., not left behind by other malware).

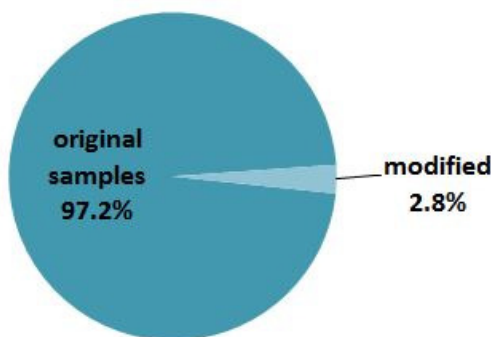


Fig. 11 –Malicious Samples – Original vs. Modified

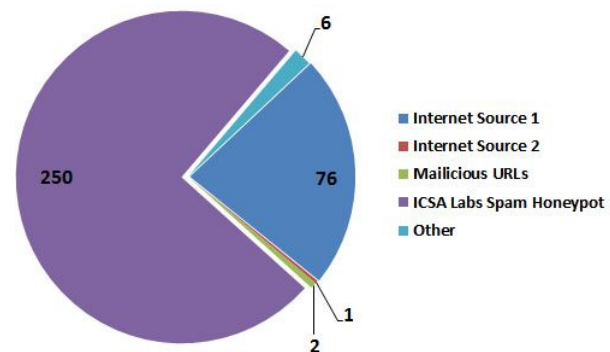


Fig. 12 – Unmodified/Non-Dropped Sample Sources

Prior ATD Reports

Following forty days of advanced threat defense testing during the 1st quarter 2017 test cycle, the Kaspersky Labs' KATA advanced threat defense solution retained ICSA Labs Advanced Threat Defense (ATD) Certification. Successful completion of this test cycle marks Kaspersky Labs' second consecutive quarter having met the [ICSA Labs ATD certification testing criteria](#).

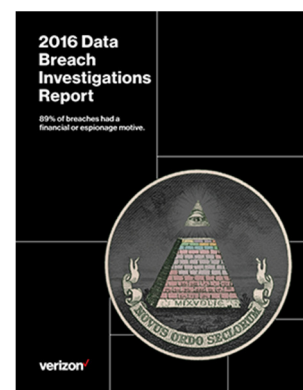
This and all earlier KATA certification testing reports can be found on the ICSA Labs web site at:

<https://www.icsalabs.com/product/kata>

Significance of the Test & Results

Readers of certification testing reports often wonder what the testing and results really mean. They ask, "In what way is this report significant?" The four statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested the Kaspersky Labs' KATA advanced threat defense solution using the primary threat vectors leading to enterprise breaches according to Verizon's Data Breach Investigations Report (DBIR).
2. ICSA Labs tests with malicious threats that other security products typically miss.
3. Kaspersky Labs' KATA demonstrated superb threat detection effectiveness against nearly 430 *new and little-known* threats.
4. The Kaspersky KATA platform had no false positives during this test cycle.

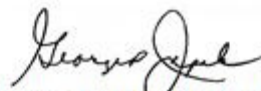


Authority



Report Date: April 5, 2017

This report is issued by the authority of the Managing Director, ICSA Labs. Tests are done under normal operating conditions.



George Japak, Managing Director, ICSALabs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 20 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

<https://www.kaspersky.com/>

Kaspersky Lab Americas Headquarters
500 Unicorn Park, 3rd Floor
Woburn, MA 01801