

Kaspersky Achieves 99.75% Detection Rate and Zero False Positives with Abusix Threat Intelligence

Industry

- ◆ Security Vendor

Background

- ◆ Kaspersky Lab is a global cybersecurity company that provides next generation security solutions and services.
- ◆ Over 400 million users and 270,000 corporate clients are protected by Kaspersky Lab technologies.

Challenges

- ◆ Kaspersky's anti-spam product development team analyzed a variety of data sources to determine the best way to get continuous real-time access to high quality and comprehensive network abuse data.
- ◆ Although Kaspersky has many existing sources of abuse data, including its own spam traps and spam exchange, customer data, and partner feeds, the company's endpoint security experts quickly realized they also needed Abusix Data Services to ensure the highest levels of anti-spam quality and accuracy.

Solution

- ◆ Kaspersky chose Abusix Data Services because of the size, quality, and real-time delivery of spam and abuse data.
- ◆ Kaspersky uses Abusix's abuse data to continuously tune its anti-spam detection algorithms and Abusix's technical headers to develop special rules.

Results

- ◆ Abusix's high quality feeds enable Kaspersky to feed data to their automatic cloud detection methods in real-time.
- ◆ Kaspersky is now able to utilize several times more data as it refines its filters and detection mechanisms.
- ◆ Abusix threat intelligence has improved Kaspersky's detection algorithms, providing their customers with top quality anti-spam protection.

The Customer

Kaspersky Lab is a global cybersecurity company that provides next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and they help 270,000 corporate clients protect what matters most to them.

The Situation

Spam email has become an important malware distribution channel leading to virus outbreaks, security breaches, and jeopardizing confidential personal and corporate information. Kaspersky Lab has built a strong business providing enterprises and consumers with the ability to catch spam and filter malware before they create problems in their customers' networks.

A critical piece of building effective anti-spam products is to train the software's algorithms on existing abuse data. Kaspersky's anti-spam product development team analyzed a variety of data sources to determine the best way to get continuous real-time access to high quality and comprehensive network abuse data.



Detection Rate



False Positives

The Solution

Although Kaspersky has many existing sources of abuse data, including its own spam traps and spam exchange, customer data, and partner feeds, the company's endpoint security experts quickly realized they also needed Abusix Data Services to ensure the highest levels of anti-spam quality and accuracy. Darya Loseva, Kaspersky Lab's head of content analysis and research, said, "We chose Abusix Data Services because of the size, quality, and real-time delivery of spam and abuse data."

Kaspersky uses Abusix's abuse data to continuously tune its anti-spam detection algorithms and Abusix's technical headers to develop special rules. Loseva added, "Abusix's data is of such high quality that we are able to feed our automatic cloud detection methods in real-time. Abusix has earned our complete and total trust."

THE SITUATION

-  High Demand for Testing Security Vendor Products
-  Need for a real-time corpus of spam messages
-  Need for Quality and Relevant Data

THE PARTNERSHIP

-  High Quality and Accurate Data
-  Better testing parameters
-  Improved Security Products

THE RESULTS

-  Diverse Testing Parameters
-  Greater Result Accuracy
-  Improved Overall Trust

The Results

The results have been impressive. Loseva credits Abusix with helping improve Kaspersky's detection algorithms and providing their customers with top quality anti-spam protection. Using Abusix threat intelligence feed as their data source, Kaspersky Linux Mail Security 8.0 won the VBSpam+ award in the latest Virus Bulletin with a detection rate of 99.75% and zero false positives.

And since Abusix is able to provide a huge quantity of messages, Kaspersky is now able to utilize several times more data as it refines its filters and detection mechanisms.



"The cooperation with Abusix has been wonderful. Using Abusix Data Services as our data source, Kaspersky Linux Mail Security 8.0 won the VBSpam+ award in the latest Virus Bulletin with a detection rate of 99.75% and zero false positives. That is awesome."

- KASPERSKY LABS