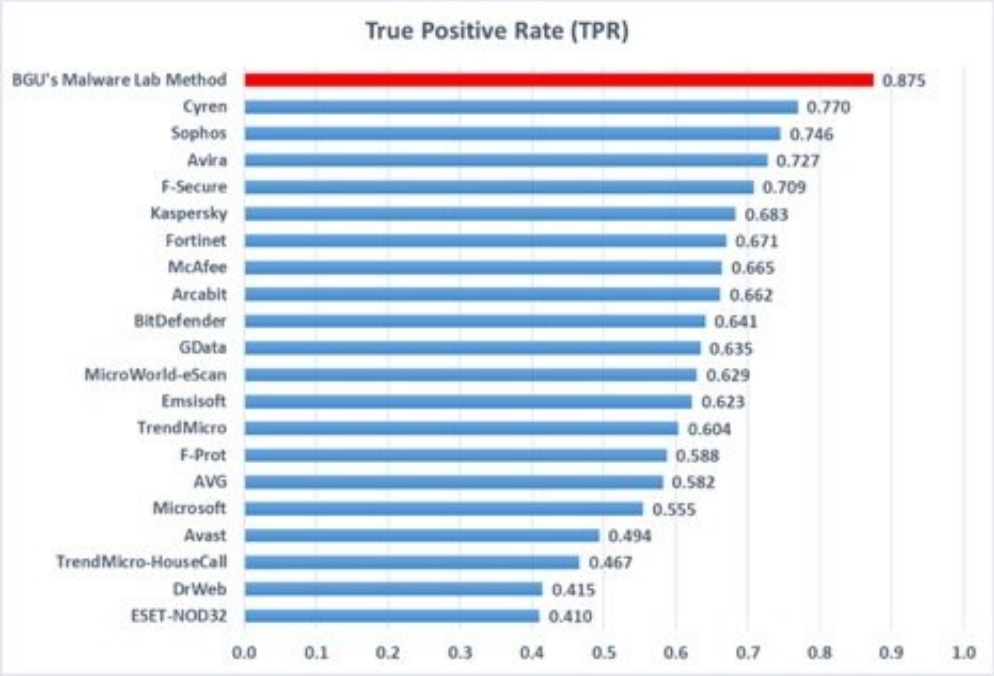
New malicious email detection method outperforms 60 antivirus engines

July 19 2018



Ben-Gurion University researchers compared their detection model to 60 industry-leading antivirus engines as well as previous research, and found their system outperformed the next best antivirus engine by 13 percent -- significantly better than such products including Kaspersky, MacAfee and Avast. Credit: Ben-Gurion U. cyber@bgu

Ben-Gurion University of the Negev (BGU) Malware Lab researchers have developed a new method to detect unknown, malicious emails that is more accurate than the most popular antivirus software products.

Email messages are widely used by attackers to deliver dangerous content to a victim, such as attachments or links to malicious websites.

"Existing email analysis solutions only analyze specific email elements using rule-based methods, and don't analyze other important parts," says Dr. Nir Nissim, head of the David and Janet Polak Family Malware Lab at Cyber@BGU, and a member of the Department of Industrial Engineering and Management. "Moreover, existing antivirus engines primarily use signature-based detection methods, and therefore are insufficient for detecting new, unknown malicious emails."

This method, called Email-Sec-360°, was developed by Aviad Cohen, a Ph.D. student and researcher at the BGU Malware Lab. The research, published in the exclusive scientific journal *Expert Systems with Applications*, is based on machine learning methods and leverages 100 general descriptive features extracted from all email components, including the header, body and attachments. The methodology does not require internet access, so it can be deployed by individuals and organizations, and it provides enhanced threat detection in real time.

For their experiments, the researchers used a collection of 33,142 emails (12,835 malicious and 20,307 benign) obtained between 2013 and 2016. They compared their detection model to 60 industry-leading antivirus engines as well as previous research, and found their system outperformed the next best antivirus engine by 13 percent—significantly better than such products including Kaspersky, MacAfee and Avast.

"In future work, we are extending our research and integrating analysis of attachments such as PDFs and Microsoft Office documents within Email-Sec-360°, since these are often used by hackers to get users to open and propagate viruses and malware," Dr. Nissim says. "These analysis methods have already been developed by the David and Janet Polak Family Malware Lab at BGU."

The Malware Lab researchers are also considering developing an online system that evaluates the security risk posed by an email message. It would be based on advanced machine learning methods and allow users worldwide to submit suspicious email messages and instantly obtain a maliciousness score and a recommendation on how to treat the email. In addition, the system would assist in collecting benign and malicious emails for research purposes which, due to privacy issues, is currently a very difficult task for researchers in this arena.

More information: Aviad Cohen et al, Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods, *Expert Systems with Applications* (2018). DOI: 10.1016/j.eswa.2018.05.031

Provided by American Associates, Ben-Gurion University of the Negev