False Positives

Myths, Mystery, and Mastery

CYLANCE™

As leading cybersecurity-conscious enterprises evaluate endpoint security alternatives, several key metrics have emerged to help evaluate risk. Chief among these metrics is the efficacy ratio – the measurement of how effective a solution is in preventing malware from attacking an IT infrastructure. Keen-eyed executives also monitor the false positive ratio. The SANS Institute, which provides IT industry information, security training, certification, and research, defines this notion thusly: *A false positive is any normal or expected behavior that is identified as anomalous or malicious.*[1]

At first glance, false positives can have a detrimental effect on worker productivity when a piece of benign utilitarian software is errantly blocked. At minimum, this can cause work interruption, but often results in subsequent help desk calls and hours of remediation work by the IT team. In extreme cases[2], a false positive can have serious security implications for the organization.

Knowing this, signature-based antivirus vendors often try to spin false positive rates to favor their offering because by design, blacklisting technologies only block known bad. But how can any forthright vendor weave this tangled web?

1. https://www.sans.org/security-resources/idfaq/what-is-a-false-positive-and-why-are-false-positives-a-problem/2/8

2. http://www.theregister.co.uk/2010/04/21/mcafee_false_positive/

The Fallacy of Binary Whitelisting

As Patrick Bayle points out in a recent blog post, objectivity is a matter of understanding and occasionally reframing the parameters. As an example of this, please follow the logic in the decision tree in Figure 1 below.

This framework would categorize *MS Power Tools* as a 'potentially unwanted program' and as such, block it.

As PC World points out, *Some antivirus products share the same detection engine or malware signatures. This is the result of inter-vendor partnerships that regular users are often unaware of. So what appears as a malware detection by three separate products in VirusTotal could actually be the result of a single bad signature shared by all of them.*[3]

Many signature-based antivirus vendors would not classify MS Power Tools as a PUP due to the binary nature of signature-based systems, and as such, would completely block an instance of this software. This would indeed cause frustration with users (in this case, likely a set of power users) who might otherwise legitimately use the software for non-nefarious purposes.

There Has To Be a Better Way...

To balance the need to access information with the desire to protect it, risk management teams favor solutions with excellent efficacy while providing flexibility. Forward-thinking security practitioners are seeking solutions outside of traditional signatures, behavioral, and heuristic approaches to achieve that balance. A new data science approach has recently emerged that leverages the power of artificial intelligence and machine learning. CylancePROTECT® is just such a solution. CylancePROTECT boasts an efficacy rate of over 99% against malware and a miniscule false positive rate of .000314%. Thousands of customers have arrived at this conclusion, not by reading a white paper such as this, but by testing for themselves in their own environments. Click here to learn more about CylancePROTECT, or to understand how CylancePROTECT compares to signature-based antivirus, please visit testmyav.com.

3. http://www.pcworld.com/article/2883692/virustotal-tackles-false-positive-malware-detections-plaguing-antivirus-and-software-vendors.html

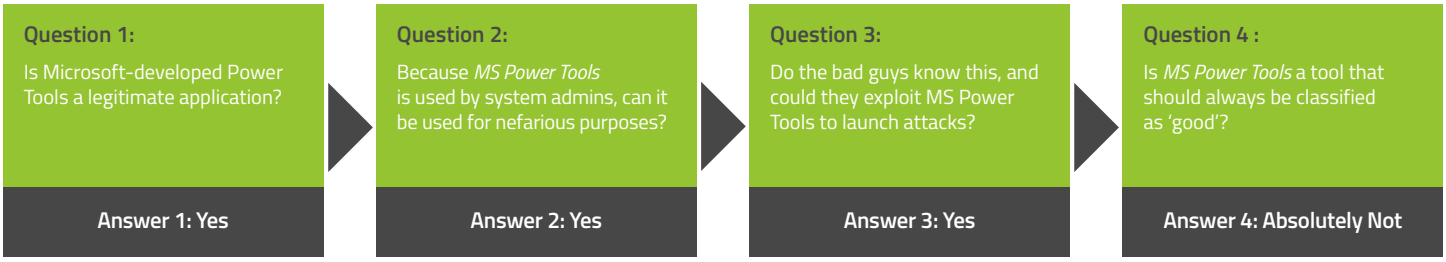

Figure 1

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

20170309-0564