Root cause analysis - Web protection false positive

Malwarebytes Engineering and Research

January 27, 2018

Introduction

The purpose of this Root Cause Analysis is to determine the causes that contributed to the release of a protection update that resulted in some customers experiencing many website “block” messages and excessive RAM usage.

Event Description

On the morning of Saturday, January 27th, 2018 protection update v1.0.3798 was released for all versions of Malwarebytes for Windows. As endpoints updated to this release, customers noticed their machines were reporting many Internet block notifications, and a sudden large increase in RAM usage.

Malwarebytes was immediately notified via our Customer Success team, who notified Engineering and Research. We immediately shut off updates to all customers to limit the number of endpoints that were affected. A review of recent updates found that we had included in the Web Filtering Block List a detection with a syntactical error that resulted in the Web Filtering System to block a large range of IPs.

This broken detection was present in the update version v1.0.3798 thru v1.0.3802. (v2018.01.27.03 - v2018.01.27.11 for MBES customers). It was removed in v1.0.3803 (v2018.01.27.12 for MBES customers).

The event could have affected customers running any version of the following products:

- Malwarebytes for Windows Premium
- Malwarebytes for Windows Premium Trial
- Malwarebytes Endpoint Security (MBES)
- Malwarebytes Endpoint Protection (Cloud Console)

Malwarebytes products **not** effected:

- Malwarebytes for Windows in Free Mode
- Malwarebytes for Mac
- Malwarebytes for Android
- ADWCleaner
- Malwarebytes Incident Response standalone (MBBR)
- Malwarebytes Incident Response (Cloud Console) for Windows or Mac

This investigation will result in identification and implementation of changes to the release process of these detections, specifically – but not limited to – stricter verification and validation of detection syntax and scope.

Chronology of Events

All these occurred on the morning of Saturday January 27, 2018, and all times are Pacific Standard Time (PST).

Time	Event
07:40 AM	**V1.0.3798** was posted to the update server. This update contained a Web Filtering detection that would cause our Web Filtering platform to block all connection attempts between 128.0.0.0 and 191.255.255.255. (The version for our MBES customer was **v2018.01.27.03**)
07:55 AM	This issue was first reported to our Research Team.
07:56 AM	The Research Team immediately put our update system into “maintenance mode”. This is the standard response to False Positive reports, which stops the flow of potentially bad updates.
07:56 to 10:48	While the update system was disabled, all recent changes to the detections were backed out and analyzed. Several versions were posted during this time for internal testing purposes. Once we were sure this issue was fixed, our QA Team approved it for release.
10:48 AM	The update **v1.0.3803** without the bad detection was posted. (The version for our MBES customers was **v2018.01.27.12**)

Findings and Root Cause

There are detection syntax controls in place to prevent such events as the one experienced in this incident. Recently we have been improving our products so that we can show the reason for a block, i.e. the detection "category" for the web protection blocks. In order to support this new feature, we added enhanced detection syntaxes to include the block category in the definitions. The unfortunate oversight was that one of the syntax controls was not implemented in the new detection syntax, which cause the malformed detection to be pushed into production.

Corrective Action

Based on the finding listed above, the following corrective actions will be taken:

- The system that performs the syntax checking of all Web Filtering heuristics will be expanded to reject entries that cover these wide IP ranges.
- The components within the Malwarebytes Web Filtering system that runs on customer computers will be changed to perform stronger checking of these entries – similar to the point above – and reject any that do not meet that criteria.
- Improve the facility within our publishing system that provides the ability for faster rollback of problematic detections. This will reduce the window of exposure, thus reducing the number of customers impacted.
- Add many more computers to our existing testing cluster to increase the scope of our coverage.