Improving the Safety of Malwarebytes Updates

Malwarebytes Research and Engineering

January 31st, 2018

Purpose

This document describes how Malwarebytes Research and Engineering is responding to the incident that occurred on the morning of January 27th, 2018. On this morning, a protection update was released that caused our Web Protection System to block a wide range of IP addresses, causing outages and system instability for some of our customers.

This plan shows the areas that will be addressed, gives the current state of those areas, then lists the steps that are planned to improve those areas. Finally, an estimate of the timeframe to deploy those improvements are also given. The content of this document as well as the timeframes are subject to change.

The following are actions have been completed or are planned by Malwarebytes Research and Engineering:

Enhanced IP Syntax Checking before Publication

Issues that will be prevented

- Badly-formed IP addresses allowed onto the endpoint, causing unexpected Web Protection blocks
- Unintended blocking of wide ranges of IPs or top-level domains
- Unexpected high memory or CPU usage on the endpoint

Current Prevention Techniques

- Syntax checking to verify all are correctly formatted

Planned Prevention Techniques

- Further limiting CIDR ranges to between 24 and 32
- Expanded total count of blocked IPs are within realistic range

Engineering Plan

- Planned Validations:
    - All IPs are correctly formatted
    - CIDR ranges between 24 and 32 only
    - Total count of IPs in the expanded list cannot exceed a certain range
- Changes are required to the build system, the workflow manager and several utility programs that handle and route the IP block lists

Deployment Timeframe

- Completed on January 30th, 2018

Enhanced Malwarebytes Web Filtering Runtime Syntax Checking

Issues that will be prevented

- Badly-formed IP addresses used by the endpoint, causing unexpected IP blocks
- Unintended blocking of wide ranges of IPs
- Unintended blocking of non-malicious IP addresses
- Unexpected high memory or CPU usage on the endpoint

Current Prevention Techniques

- Syntax checking to verify all are correctly formatted

Planned Prevention Techniques

- Validate IP address and CIDR range before usage, and reject if improperly formed
- To prevent excessive memory usage, do not expand the IPs into individual IPs, but keep them in a hashed CIDR format
- Verify no block attempts on any Malwarebytes service

Deployment Timeframe

- March 1st, 2018

Rollback Support within the Publishing System

Issues that will be prevented

If all the other preventive measures fail to detect a harmful protection update, ensure a quick rollback of to a known-safe version would greatly reduce the number of endpoints that are affected

Current Prevention Techniques

- The current technique is a process that can take from 30 minutes to 3 hours

Planned Prevention Techniques

- A new process where a “rollback” is created beforehand, tested and is made available in the “chamber” for immediate release
- If a harmful update is detected, Malwarebytes Research can release the “rollback” update in **seconds**
- This will roll all our customers back to a safe protection update that is >24 hours old
- Once the issues are fixed, a new protection update will be released that will bring all customers to a current protection state
- This technique will apply to all versions of Malwarebytes for Windows

Deployment Timeframe

- February 28th, 2018

Malwarebytes Endpoint Protection Agent Startup Sequence

Issues that will be prevented

For our business customers running Malwarebytes Endpoint Protection, in the cases where a harmful detection is blocking its ability to get updates, this approach would allow our customers a route to shut off offending protection features from the management console, long enough to get the endpoint fixed.

Current Prevention Techniques

- Customers must shut off protection from the console and then reboot the endpoints. Because of the non-deterministic order that the protection systems start up, this approach will work in most situations, but not all.

- Or they need to access the endpoint and shut off Malwarebytes, delete the harmful update files, then restart Malwarebytes. This technique usually works, but requires the customer to visit every endpoint.

Planned Prevention Techniques

- On startup, if the Endpoint Protection systems cannot connect to the cloud servers for the purpose of retrieving a policy update, it will attempt a series of steps to obtain the policy, then apply any policy changes. If all attempts fail, it will fall back to its most recent last-known-good policy.

Deployment Timeframe

- March 8th, 2018

Enhanced False Positive Testing before Publishing

Issues that will be prevented

By expanding the testing of the Web Protection System before the protection updates are published, we can prevent the Web Protection System from detecting most of the popular websites and non-routable IP addresses.

Current Prevention Techniques

- Checking against a list of known-good websites

Planned Prevention Techniques

Before publishing protection updates, perform the following checks:

Validate that the **Domain Block List** does not block any of the following:

- Domains from a vastly-expanded list of known-good websites
- Domains that Malwarebytes uses for updates or telemetry

Validate the **IP Block List** does not contain:

- Non-routable IP addresses (private IP address space)

Deployment Timeframe

- March 15th, 2018

Allow Endpoint Protection Customers to Control Update Timing

Issues that will be prevented

Most customers have asked for the ability to specify longer intervals between updates, or to specify that updates occur at a certain time-of-day, for better prediction of change. Some customers have asked for the ability to select an “aging period” that delays the applying of protection updates until they have been “in the wild” for a few hours.

These new features would provide our Endpoint Protection customers a policy-level setting where they could select the timing of when updates are applied, giving them finer control over changes on their endpoints.

Current Techniques

- Updates are released ~10x per day. The Endpoint Agent checks for updates every hour, then downloads and applies them automatically without delay.

Planned Techniques

- Allow user to specify intervals or delays for applying protection updates, for example:
    - Apply all protection updates on a set interval (e.g. daily, or at a time-of-day)
    - Disable protection updates entirely (e.g. for emergencies or testing)
    - Apply protection updates only after they are “aged” (e.g. x hours old)

Deployment Timeframe

- Initial functionality: April 12th, 2018
- Complete functionality: June 7th, 2018