Improving the Safety of Malwarebytes Updates

Malwarebytes Research and Engineering

January 31st, 2018
Updated August 3, 2018

Purpose

This document describes how Malwarebytes Research and Engineering has responded 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 taken to improve those areas. 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

Prevention Techniques before Incident

- Syntax checking to verify all are correctly formatted

Additional Techniques Completed

- Further limiting CIDR ranges to between 24 and 32
- Where possible, eliminated the need to expand the number of blocked IP into individual IP addresses, otherwise limited the expansion of blocked IPs to a realistic count

Deployment Timeframe

- Completed in January 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

Prevention Techniques before Incident

- Syntax checking to verify all are correctly formatted

Additional Techniques Completed

- 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

- Completed in March 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

Prevention Techniques before Incident

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

Additional Techniques Completed

- Malwarebytes Research has created a process where a "rollback" is created for every Protection Update. It is tested and then made available in for immediate release if needed
- 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 at least 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 process takes between 1 and 3 hours.
- This technique will apply to all versions of Malwarebytes for Windows

Deployment Timeframe

- Completed in March 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

- Q4 of 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.

Prevention Techniques before Incident

- Checking against a list of known-good websites

Additional Techniques Completed

The following checks are performed before publishing protection updates:

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

- Domains from the top 500 from Alexa
- 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

- Completed in March 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 immediately downloads and applies them automatically.

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

- Changes to the Malwarebytes updating backend systems have been completed and are under testing.
- Settings that support this feature in the Endpoint Protection product are planned for later this year.