**Playbook Guide:**

**Malware Outbreak**

August 1, 2018 – Revision A

# Introduction

LogRhythm Case Playbooks are designed by the LogRhythm Threat Research Team to make it easier and more repeatable for analysts to respond to incidents. Through the rich feature set of Case Playbooks, analysts can not only create their own playbooks, but modify existing playbooks, as well as attach company policies and procedures in the playbook. All of these features allow the analyst to react faster and more efficiently, decreasing the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

This guide describes the Malware Outbreak Playbook, and how to configure the playbook. An Analyst should use this playbook when responding to multiple malicious events.

The Malware Outbreak Playbook is built on industry recommended practices for identifying Malware Outbreaks. The Playbook helps an analyst track, and capture evidence. Using this playbook, you should have sufficient evidence in your case to report for compliance (e.g. HIPAA or GDPR), and/or begin legal action if the actor or actors were identified.

# Prerequisites

* This playbook requires Web Console and LogRhythm Enterprise 7.4 and later.

# Import the Playbook (One Time Only)

To import a Playbook:

1. Download the playbook from the shareables section of Community.
2. Log in to the Web Console as a user with rights for creating and maintaining playbooks
3. Select Administration and Playbooks.
4. Select Import Playbook.
5. Browse to the Playbook named “Playbook-MalwareOutbreak.pbe” and click on “Open”.
6. Click on “Import” to complete the action.

# Use the Playbook

1. Create a new case or open an existing case.
2. Within the case, click on “Add Playbooks”.
3. Use the drop-down menu to select the Malware Outbreak playbook or click on “Advanced” to select multiple playbooks.
4. Under Playbooks, expand the playbook procedures.
5. Expand each procedure and assign the procedure, add notes to the procedure, add a due date to the procedure, as needed.
6. Skip or close the procedure by putting a check in either the skip or close box and adding appropriate notes.

**Malware Outbreak Playbook Procedures**

The playbook is a set of 9 procedures, ranging from initial investigation, to creating an incident, and the steps needed to complete the investigation. There are some details that will help an analyst action a more advanced procedure. The procedures included are:

1. Determine if you are investigating an incident or event
2. Determine if the malware is a false positive
3. Acquire, preserve, secure, and document evidence
4. Isolate the subnet in which malware outbreak is occurring
5. Disable the affected user accounts
6. Isolate the infected hosts
7. Perform forensics on hosts
8. Re-image the host systems
9. Provide feedback and lessons learned to reduce chances of incident occurring again

### © LogRhythm, Inc. All rights reserved

This document contains proprietary and confidential information of LogRhythm, Inc., which is protected by copyright and possible non-disclosure agreements. The Software described in this Guide is furnished under the End User License Agreement or the applicable Terms and Conditions (“Agreement”) which governs the use of the Software. This Software may be used or copied only in accordance with the Agreement. No part of this Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than what is permitted in the Agreement.

### Disclaimer

The information contained in this document is subject to change without notice. LogRhythm, Inc. makes no warranty of any kind with respect to this information. LogRhythm, Inc. specifically disclaims the implied warranty of merchantability and fitness for a particular purpose. LogRhythm, Inc. shall not be liable for any direct, indirect, incidental, consequential, or other damages alleged in connection with the furnishing or use of this information.

### Trademark

LogRhythm is a registered trademark of LogRhythm, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or service marks of their respective holders.