

# Table of Contents

|                                                   |           |
|---------------------------------------------------|-----------|
| Table of Contents.....                            | 2         |
| <b>Introduction.....</b>                          | <b>7</b>  |
| <b>Components.....</b>                            | <b>8</b>  |
| <b>Persistence via Runkeys.....</b>               | <b>11</b> |
| <b>Persistence via Process Creation.....</b>      | <b>13</b> |
| <b>Detection.....</b>                             | <b>16</b> |
| <b>Service Detection.....</b>                     | <b>25</b> |
| <b>Reinfection Downloading from Internet.....</b> | <b>34</b> |
| <b>Reinfection Recreating Stored File.....</b>    | <b>40</b> |
| How to Store an EXE in the Registry.....          | 41        |
| Retrieving the File from the Registry.....        | 44        |
| Why This Matters.....                             | 44        |
| <b>Adding Antidebugging Techniques.....</b>       | <b>45</b> |
| Summary:.....                                     | 47        |
| Proof of Concept.....                             | 47        |
| <b>Exercise.....</b>                              | <b>48</b> |
| Challenge: Why Redetection Happens.....           | 49        |
| How to Avoid Triggering Detection Again.....      | 49        |
| Why It Works.....                                 | 50        |
| <b>Conclusions.....</b>                           | <b>50</b> |