Playbook – Malicious Code (Malware)

**<Insert Corporate Logo>**

**Document Version** 1.1 **Date**

**Change Log**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Change |
| 3/12/2016 | 1.0 | Josh Geno | Complete rebuild from prior “top-down” format. Re-written into flowchart format with detailed instructions in playbook doc |
| 8/14/2018 | 1.1 | Josh Geno | Changed to generic tool/process/department references; updated resources that have changed versions or have been superseded |
| 10/2/2018 | 1.2 | Josh Geno | Added Instructions for BIOS/UEFI rootkits |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Introduction 4](#_Toc526511377)

[License 4](#_Toc526511378)

[Incident Lifecycle 5](#_Toc526511379)

[Prepare 6](#_Toc526511380)

[A1 6](#_Toc526511381)

[A2 7](#_Toc526511382)

[A3 8](#_Toc526511383)

[A4 8](#_Toc526511384)

[A5 9](#_Toc526511385)

[A6 10](#_Toc526511386)

[Detect 11](#_Toc526511387)

[B1 – B11 11](#_Toc526511388)

[B12 12](#_Toc526511389)

[B13 - B15 13](#_Toc526511390)

[Triage / Prioritize 14](#_Toc526511391)

[Note Regarding Rapid Assessment Methodologies 14](#_Toc526511392)

[Checkbox Assessment 14](#_Toc526511393)

[Weighted Assessment 15](#_Toc526511394)

[C1 – C8 16](#_Toc526511395)

[C9 – C15 17](#_Toc526511396)

[C16 - C18 18](#_Toc526511397)

[C19 19](#_Toc526511398)

[Analyze 19](#_Toc526511399)

[D1 19](#_Toc526511400)

[D2 20](#_Toc526511401)

[D3 21](#_Toc526511402)

[D4 21](#_Toc526511403)

[D5 22](#_Toc526511404)

[D6 23](#_Toc526511405)

[D7 24](#_Toc526511406)

[Contain/ Eradicate/ Recover 25](#_Toc526511407)

[E1 & E2 25](#_Toc526511408)

[E3 26](#_Toc526511409)

[E4 27](#_Toc526511410)

[E5 28](#_Toc526511411)

[E6 29](#_Toc526511412)

[E7 30](#_Toc526511413)

[E8 & E9 31](#_Toc526511414)

[E10 32](#_Toc526511415)

[E11 33](#_Toc526511416)

[E12 – E14 34](#_Toc526511417)

[E15 35](#_Toc526511418)

[E16 35](#_Toc526511419)

[E17 36](#_Toc526511420)

[E18 – E20 37](#_Toc526511421)

[E21 37](#_Toc526511422)

[E22 38](#_Toc526511423)

[E23 38](#_Toc526511424)

[E24 38](#_Toc526511425)

[Post-Incident 39](#_Toc526511426)

[F1 39](#_Toc526511427)

[F2 40](#_Toc526511428)

[F3 40](#_Toc526511429)

[F4 40](#_Toc526511430)

[F5 41](#_Toc526511431)

[F6 41](#_Toc526511432)

# Introduction

This playbook is the text compendium to the Malicious Code (Malware) response flowchart.

It provides needed details, explanations, and external resource links for the various components called out in the flowchart. This guide and flowchart are not intended to serve as a full Security Incident Framework or response process, it contains components specific to malicious code response.

To maximize the value of the response flowchart and this guide, it must be modified to reflect your organization’s incident response process/framework, the roles and responsibilities of individuals in your organizational structure, security tools, and TTPs (Tactics, Techniques, and Procedures) present in your environment.

This Playbook can be automated by most incident management platforms. Incident management platforms that can also automate information collection from security tools will be of particular value during an actual incident.

For the purposes of this document, malware includes all forms of malicious code, such as viruses, worms, rootkits, booktkits, adware, remote access toolkits, droppers, launchers, reverse shells, vulnerabilities, keyloggers, crypto miners, spam generators, botnets, maldocs, etc. Even though ransomware is malware/malicious code, it is treated in a separate playbook.

Malware authors have decades of prior art to drive innovations today. Be prepared.

The author is assumes no liability for the content, quality, relevance, fitness for purpose, or accuracy of any materials used in this document and assumes no liability for any real or potential harms associated with use of the document or flowchart.

## License

This work is licensed under  [Creative Commons Attribution-ShareAlike 4.0](https://creativecommons.org/licenses/by-sa/4.0/)

https://creativecommons.org/licenses/by-sa/4.0/

**Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

**ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

**No additional restrictions** — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Copyright 2016 Joshua C Geno

# Incident Lifecycle

This malware response guide uses a standard incident lifecycle including preparations to prevent, detect, and respond to a malware threat. Post-incident lessons learned are fed back into the lifecycle as continuous improvement measures.

Again, the flowchart and guide are not meant to capture the entire incident response function, only those components specific to detection and response for a malware incident. For a full IR framework, reference SANS Incident Handlers Handbook, Carnegie Mellon’s Handbook for Computer Security Incident Response Teams, or ENISA’s Good Practice Guide for Incident Management.

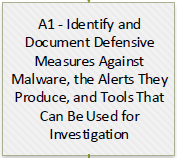


# Prepare



The prepare phase includes activities and protective measures that should be put in place prior to an incident. It also includes activities and protective measures incorporated from post-incident activities following an incident.

The more time analysts and engineers spend in prepare, the less time they’ll spend in response when an actual malware incident happens.



A1 - In this step the organization should take a close look at their inventory of security and infrastructure tools that can detect malware or aid the investigation of a malware incident. Look at the threat carefully from a defenders point of view. (blue team) Document these tools and a few samples of the type of alert or notification that can be expected. Document sample investigation queries/reports/etc. that engineers can run for each tool with ‘how to’ instructions so there is a quick reference during an incident. Collect any supporting information (network diagrams, crown jewel assessments, asset inventory, etc.) that will help with decisions during an incident and regularly update them.

This information can then be called out in multiple phases:

* Later in the prepare phase to fill gaps and bolster response capabilities
* The detect phase as a feed-in for threat indicators/alerts
* The analyze phase as tools to help positively ID the malware
* The contain/eradicate/recover phase as tools to help isolate bad code or infected systems; remove malicious code, or blocking malicious network traffic.

In all phases the output of one tool, such as a hash of the malware executable, can be used to enrich or correlate information in other tools. This will be highly dependent on the tools your organization has implemented and the level of automation between the tools.

Don’t forget to include non-technical alerts, such as user reports or external notifications from business partners or law enforcement.

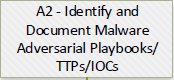
Resources:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 36)

<https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5BNASA%20Information%20Security%20Incident%20Management%5D.pdf> (page 44)

<https://www.owasp.org/index.php/OWASP_Anti-Malware_-_Knowledge_Base>

<https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM_English_Pack.zip> (IRM 1 and 7)



A2 - This step is about looking at the malware threat from the attacker’s point of view. (red team)

The more responders understand how the organization can be attacked the better they can fill gaps, tune security tools and procedures, and the better they can respond to an attack. Collect and share adversarial playbooks from actual attacks. Research TTPs related to malware. Collect IOCs (Indicators of Compromise) and search for them in the environment.

Verizon releases an annual data breach report that contains details of actual attacks. It is an excellent source of adversarial playbooks, which they call attack patterns. There are many other security researchers that release similar reports.

There are also many public sources of IOCs such as “IOCs”, FireEye’s publicly shared IOC repository. Free/Open source tools to scan the environment include Redline and Loki.

Resources:

<https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

<https://github.com/fireeye/iocs>

<https://www.fireeye.com/services/freeware/redline.html>

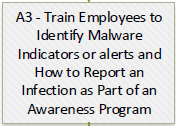
<https://github.com/Neo23x0/Loki>

<http://www.ten-inc.com/presentations/invincea1.pdf>

<https://www.owasp.org/index.php/OWASP_Anti-Malware_-_Knowledge_Base>

<https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM_English_Pack.zip> (IRM 1 and 7)

<https://news.sophos.com/en-us/2013/11/01/how-malware-works-anatomy-of-an-attack-in-five-stages-infographic>



A3 - If your organization has not already done so, implement an awareness program and include malware training as part of that awareness program. At minimum, every person in the company should be aware of basic indicators of malware/ransomware infection and know how to report it to IT security. The program should also stress the avoidance of clicking unknown links or opening email attachments that they were not previously expecting.

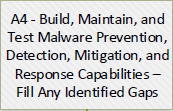
Resources:

<https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf>

<https://insights.sei.cmu.edu/insider-threat/2017/06/security-awareness-and-training-part-9-of-20-cert-best-practices-to-mitigate-insider-threats-series.html>

<https://www.csoonline.com/article/2133408/data-protection/network-security-the-7-elements-of-a-successful-security-awareness-program.html>

<https://www.wombatsecurity.com/blog/security-awareness-training-best-practices-to-consider>



A4 - In this stage, run tests against the previously identified security tools and TTPs to gauge detection and response capability. Make sure analysts and responders are getting expected detections and alerts. There are several sources for fake malware, such as Stackhackr or ShinoBOT. To test response capabilities, run tabletop exercises. Identify gaps in detection, alerting, and response and make plans to fill them.

Resources:

<https://stackhackr.barkly.com/builder>

<https://shinobot.com>

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 61)

<https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf>



A5 - The first time incident responders contact internal teams or external resources shouldn’t be during an actual incident. Stakeholders, such as management, other corporate teams, internal privacy/compliance, internal or external legal resources, SecaaS/incident response vendors, etc. should be regularly engaged to discuss the role they play in incident response, and regularly briefed about the Security Operations Center activities. Ideally, they should also be included in response tests or tabletop exercises.

External resources, such as local, state, or federal law enforcement are likely not able to be part of your internal response testing, but should still be considered as part of the process and called out in appropriate steps. It is beneficial to reach out to them every couple of years to maintain general awareness. They can help you understand who can help with various problems and what resources are available.

Sometimes law enforcement shows up to local security conferences or have their own security events. Make use of these opportunities.

Document stakeholders and what role they may be called to play. Communicate incident response expectations and find out what expectations they have of the SOC when requesting resources during an incident. Keep stakeholders informed as to the activities and capabilities of the SOC. See page 11 of the agoria.be document below for an example of a Skills / Responsibilities / Roles chart.

Resources:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 18)

<https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-3/preventiand-response-twopronged-approach-cyber-security-and-incident-response-planning.html>

<https://www.sans.org/reading-room/whitepapers/legal/legal-considerations-creating-incident-response-plan-37487>

<https://www.agoria.be/upload/agoriav3/Cyber-Security-Incident-Management-Guide-2015.pdf> (pages 11 and 13)

<https://www.halkynconsulting.co.uk/a/2015/12/incident-response-key-stakeholders/>



A6 – The ability to repel or recover from a malware attack hinges on your organization’s ability to maintain superior security practices.

An excellent reference for comprehensive malware prevention techniques is NIST’s Special Publication 800-83, section 3 – Malware Incident Prevention which starts on page 17 of the PDF available here: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>

At a high level, organization’s need to be able to:

* Protect computing resources and data through technical (anti-malware, IPS, etc.) and non-technical (awareness program, rule of least privilege, etc.) means.
* Have the ability to restore encrypted or corrupted data.
* Continuously reduce your organization’s attack surface. (patching, penetration testing, etc.)

Many security compliance frameworks will have these security hygiene measures documented, keep this information available and updated. If your organization does not have this documentation available, document it here for future reference.

Resources:

<https://duo.com/decipher/security-hygiene-tips-to-prevent-malware-infection-and-stop-lateral-movement>

<https://blog.malwarebytes.com/101/2016/08/10-easy-ways-to-prevent-malware-infection>

<https://support.microsoft.com/en-us/help/129972/how-to-prevent-and-remove-viruses-and-other-malware>

<https://www.makeuseof.com/tag/7-common-sense-tips-avoid-catching-malware/>

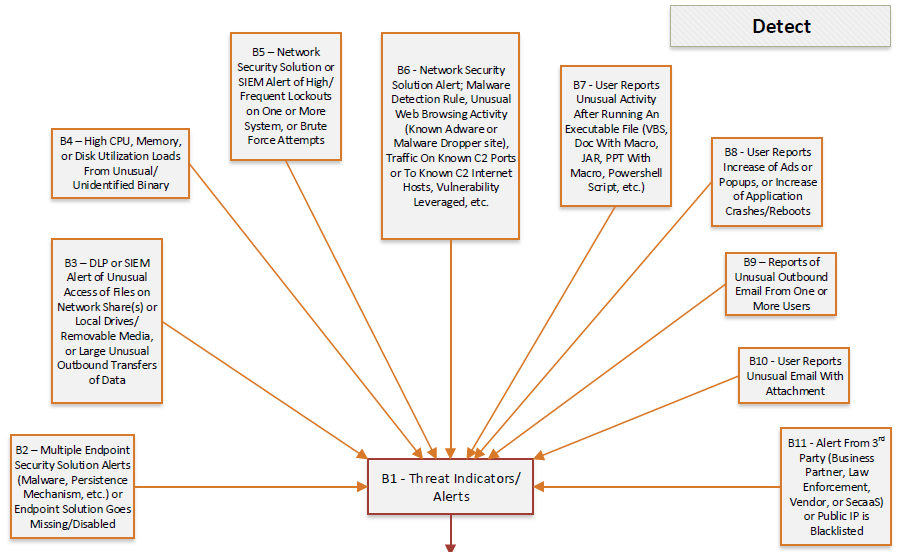
<https://www.pcworld.com/article/3156931/linux/why-malware-should-be-a-concern-for-all-linux-users-and-what-to-do-about-it.html>

<https://zeltser.com/malware-in-the-enterprise/>

<http://securityskeptic.typepad.com/the-security-skeptic/how-to-keep-spyware-off-our-enterprise-network.html>

# Detect

The detect phase covers receipt of an alert or notification and the initial data gathering to validate that an actual malware incident has occurred.



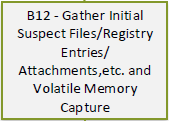
B1 – B11 – The threat indicators, technical alerts, and manual notifications identified in A1 are inputs to B1. Many of these are common among organizations and should appear in every malware playbook. Some are specific to the tools, 3rd parties, and organizational structure of a single organization. Take time to periodically review these inputs to prune or add entries as your available tools and TTPs change and make sure they all work as expected.

If the source or content of one or more of the inputs (B2 – B11) is not crystal clear to everyone on the security team, use the information identified in A1 to individually document the source and alert in this part of this document to aid responders.

Once an indicator is observed, alert is triggered, or notification is received, incident response is initiated.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 34)



B12 – Utilize the information and context available in the indicator/alert/notification to guide the initial data gathering activities. For instance, if you received an alert from a network tool that an endpoint is beaconing to a C2 internet host, use the source IP address to identify the affected endpoint. From there, use available tools to evaluate the executables running and network traffic being generated. If remote tools are not available in your environment, send someone (or acquire the endpoint) with appropriate skills to put hands on the keyboard to gather suspect registry entries, files/hashes, email attachments, web history entries, packet captures, descriptions of unusual behavior, etc.

If the cause of the indicator/alert/notification is not immediately obvious, utilize automated scripts to rapidly collect indicators, such as Bambiraptor.

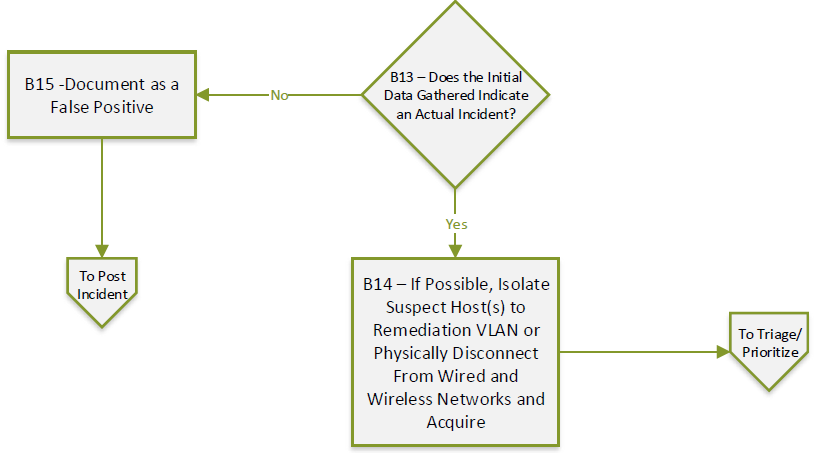
<https://www.brimorlabsblog.com/2016/12/live-response-collection-bambiraptor.html>

Gather as much information as is necessary to make a determination as to whether the indicator/alert/notification is a false-positive or an actual incident. Being familiar with malware infection and operation (A2 above) methods will help responders zero in on relevant facts quickly.

Your organization may have tools and TTPs related to gathering initial data. If so, document them here.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 34)



B13 - B15 – If there is no evidence of a malware infection after the initial data gathering and the indicator/alert/notification can be attributed to a false-positive (user observed strange behavior and called ‘just in case’, new rule from a network tool vendor, etc.), document the incident as a false positive and move to F4 in Post-Incident.

Post-Incident is still required for false-positives as documentation may need to be updated, tools may need to be tuned or rules adjusted, and stakeholders (system owners, end users) will certainly need to be told that there is no security problem.

If enough evidence has been gathered to make a determination that one or more endpoints may have a malware infection, isolate the suspect hosts. If you have remote tools isolate via remediation VLAN, or disconnect the endpoint from all wireless and wired networks and remove/unplug directly attached devices. (USB storage, IoT, PLC, printers, etc.)

Any external device that was attached should also be considered to be infected until the capabilities of the malware are known. At this stage it is likely not known exactly what family/variant of malware has infected the host(s) so the spreading mechanisms and capabilities are not yet known.

Ideally the devices physically removed from the network should be pulled and acquired by responders to prevent ‘proactive’ users from plugging them back in. A good stakeholder communication plan as part of your incident response function and a sticky note on the device or monitor (where possible) will go a long way toward keeping potentially infected devices out of the production network until the device can be acquired or remediated.

Your organization may have tools and TTPs available to remotely help with isolation to a remediation VLAN, if so document them here.

If your organization has a specific procedure for disconnecting wireless and wired network connections and physically acquiring devices, document them here.

Document your remote tools and TTPs here.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 44)

# Triage / Prioritize

The Triage/Prioritize phase covers the assessments that need to be quickly performed in order to prioritize the new/current incident in relation to other incidents already in the security incident queue.

This is also the phase where it is determined whether or not internal or external teams need to be notified of an incident. This playbook doesn’t cover the specifics of who should be contacted and what information to share with them; that is for your larger Incident Response Program to decide. This is the place we call out as appropriate to make the determination as to whether the notification portions of the Incident Response Program require action.

### Note Regarding Rapid Assessment Methodologies

The two rapid assessments below, C1 and C9, can be effectively performed two ways. Which way your organization uses will be determined by organizational needs for the level of granularity required and rate of incidents your organization handles at a time.

### Checkbox Assessment

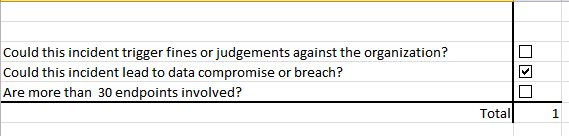
For organizations that handle few incidents at a time, an express assessment method can be used as a ‘tie-breaker’ for those few occasions where there is more than one incident in process, but there aren’t enough resources to service all of them. Each of the inputs is turned into a question and given a checkbox where it is checked if the condition is true. At the end you simply add up all the checked boxes for a score. The higher the score, the higher the priority.

Estimated number of endpoints isn’t easy to capture in a checkbox, so you have to reframe the question to “Are more than X endpoints involved?” Obviously this isn’t a one size fits all situation; you will have to come up with a number for your organization where more than that number signifies a critical situation.

The others are easy to turn into questions, such as:

* Could this incident trigger fines or judgements against the organization?
* Could this incident lead to data compromise or breach?
* Is sensitive data potentially involved?

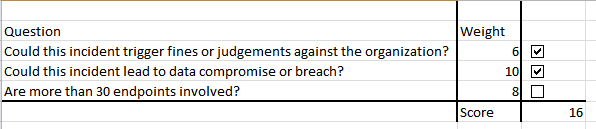
A simple spreadsheet is enough to capture responses and final score. Alternately, many case management systems allow you to setup data capture steps as part of an IR workflow.



### Weighted Assessment

For larger organizations that handle many incidents at a time and are able to run multiple responses at a time, weighted assessment provides a better level of granularity for assigning priority and the order in which incidents will be taken from the queue.

This methodology can also spark holy wars as to what weight should be given to each input. To get started stakeholders have to come together and agree on the weight of each question posed by each input. I recommend a weight of 1 -10. Invariably, one stakeholder will feel that one of the inputs, say Loss of Productivity, should be a 1 whereas a different stakeholder feels it should be a 10. However your organization gains consensus for these situations, the end goal is the same; weight each of the inputs so that when it’s question is checked, that weight is added to the total. Incidents can then be listed highest to lowest score where highest score is highest priority and will be taken by the next available responders from the queue.





C1 – C8 – The first rapid assessment concerns the organization’s expectation of potential loss due to the incident. In case the meanings of each input are not clear, here is a brief explanation of each:

* Reputation Damage – Potential for loss to repair the organization’s reputation (PR firm, advertising, etc.) May include indirect losses of lost business due to reputation damage.
* Fines/Judgements – Potential losses incurred by violating contractual agreements where there is a financial penalty, or regulatory fines.
* Loss to Replace or Repair – Potential losses incurred when systems are not available while being replaced, remediated, etc.
* Loss of Productivity – Potential loss of man-hour productivity while systems or hardware are not available for use.
* Loss Due to Legal Response – Potential loss incurred to hire lawyers, pay court fees, or potential punitive judgements.
* Loss of Competitive Advantage – Potential losses due to intellectual property or corporate secrets being leaked.

Tally the loss expectation score using the chosen assessment method above, it will be needed in C16.

Resource:

<https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model>



C9 – C15 – The second rapid assessment covers a severity assessment that will later be added to the loss assessment to determine priority. The severity assessment covers attributes of the incident itself rather than the business impact of the incident.

Additionally, it is time for responders to decide if external notifications are required or external/3rd party resources should be engaged since questions are already being asked about data compromise/breach and whether or not sensitive data is involved.

In case the meanings of each input are not clear, here is a brief explanation of each:

* Possibility of Data Compromise / Breach – Possibility that corporate data could be stolen, tampered with, or deleted. The systems involved and what function they serve should be taken into account.
* Estimated Number of Endpoints Involved – An order of magnitude assessment that is relative to the size of your business. 1 infected workstation in an organization of 10 total workstations is a much larger percent of infected hosts than 1 in a 50,000 workstation organization.
* Customer Impact – The possibility that the incident will impact your customers in some way. This could be direct financial impact or indirect impacts, such as a service being unavailable.
* Sensitive Data Involved – The possibility that protected classes of data (health, education, govt ID) or sensitive internal data (corporate secrets, intellectual property) could be affected by the incident.
* Recoverability – The relative possibility that damage caused by the incident can be reversed, rebuilt, or halted. Check the box on the checklist if recoverability is difficult, time consuming, resource consuming, or impossible.

Tally the severity assessment score using the chosen assessment method above, it will be needed in the next step. If the decision has been made that notifications are required or additional resources need to be pulled in, follow the procedures in your organization’s larger Incident Response Program to engage them.



C16 - C18 – Add the two scores calculated in C1 and C9. This is the incident’s priority score. Document this score and the two component spreadsheets from C1 and C9 in the incident documentation (Your Incident Response Program should have procedures and templates for this) and in your ticketing / case management system.

If this incident rates higher than the other items already in the queue then it takes precedence over other incidents and progresses to the Analyze phase. If it rates lower than other incidents in the queue, is added to the queue for later investigation and remediation. Any incident artifacts (data gathered, alerts, etc.) should be documented for later retrieval per your Incident Response Program’s requirements.



C19 – For incidents in the queue where responder resources have become newly available to investigate the next incident, this is the place in the playbook where the queue feeds in for malware incidents. Any malware incident in the queue will have already been through the playbook up to this point.

Responders take the incident with the highest priority score in the queue and advance it to Analyze.

# Analyze

In the Analyze phase responders will utilize internal and external resources to identify the malware, associated indicators of compromise, and its capabilities. At times it will not be possible to get a positive ID of a previously known variant of malware. In this case behavioral analysis and/or reverse engineering techniques will be employed to gather information. This information will be used in the next phase to find additional infections, close vulnerabilities, and clean infected systems.



D1 – If your security tools were able to positively ID the specific variant of malware at detection or during the initial data gathering then additional analysis to identify the infection is not necessary and responders can move to D7. Otherwise, move to D2.



D2 – To identify the specific variant of malware, indicators of compromise must be collected and compared against known variants. If the initial data gathering didn’t collect enough indicators, additional forensic data gathering may be required.

If additional systems are discovered to be infected, forensic data should be gathered from these systems as well and analyzed to make sure you are only dealing with one malware variant/infection.

Be sure to gather forensic data related to the Operating System/Software Environment (browser history, persistence mechanisms, etc.), Network (packet captures, security tool alerts/logs, etc.), and file system. (hashes of suspect executables, infected file samples, user reports of unusual activity, etc.)

Document your organization’s tools and TTPs related to D2 here.

Resource:

<https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps>



D3 – Send captured files, hashes, or download URLs to your Anti-Virus/Malware and security tool (where possible) vendors for identification. You may also be able to get a positive ID from freely available web tools, such as VirusTotal.

Document tools and TTPs related to malware ID through vendors and 3rd parties here.

Any results from these tools should be stored with incident artifacts per your Incident Response Program requirements.

Resources:

<https://www.virustotal.com/#/home/upload>

<https://www.hybrid-analysis.com/>

<https://virusscan.jotti.org/en>

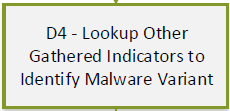
<https://www.threatminer.org/>

<https://valkyrie.comodo.com/>

<https://metadefender.opswat.com/#!/scan-file>

<https://n0where.net/incident-response-malware-analysis-irma>

<http://www.herdprotect.com/knowledgebase.aspx>



D4 – In tandem with D3, search the internet for any unique artifacts or indicators. A windows registry entry or oddly named android APK can sometimes lead to a write-up by a security vendor that identifies one specific malware variant.

Any findings should be documented per your Incident Response Program requirements.

Resource:

[www.google.com](http://www.google.com)



D5 – If you’ve leveraged all of your organization’s TTPs, your security tool vendor’s resources, and exhausted relevant public resources, you may be up against a new or rare variant of malware that has not been identified yet. If you have an ID, skip this step.

To find out how it initially infects/utilizes a dropper, operates, persists within a system, spreads to other systems, and communicates with its creator, you are going to have to employ behavioral analysis and/or reverse engineering. Without this information you will not be able to effectively contain, eradicate, and recover in the next step.

Not every organization has someone on staff who possesses these capabilities. If this is the case in your organization, you should escalate this need to management and recommend contracting with a 3rd party or security tool vendor who can offer a service level agreement appropriate to the criticality of an unidentifiable malware infection in your organization.

Some security tool vendors offer behavioral analysis/reverse engineering as part of their service contract for the tool, though, there typically isn’t a service level agreement when this is the case and cannot be relied upon for a quick turn-around during a security incident.

There are automated behavioral analysis and reverse engineering products on the market, this may make the most sense for your organization. Keep in mind, however, that these products can only identify operations that their programmers built into them. They may not be able to identify truly new/unique malware capabilities.

Document your organization’s tools and TTPs related to malware behavioral analysis and reverse engineering here.

Any findings from the tools or manual reverse engineering activities should be formatted as a write-up and be documented as part of your incident artifacts.

Resources:

<https://www.reverse.it>

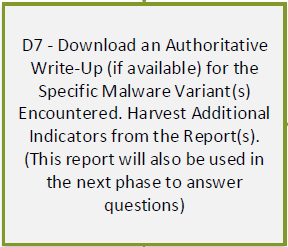
http://struppigel.blogspot.com



D6 – By this step we should have either reached a positive ID of the malware, or know enough about its operation from behavioral analysis/reverse engineering to know whether or not the malware sample encrypts files and holds them ransom.

If it does have the capability, whether or not it has actually encrypted anything yet, it is ransomware and the incident should continue with the Ransomware playbook. Run it from the start to make sure you don’t miss anything. The incident is done with the Malicious Code (Malware) playbook.

If it does not hold files for ransom, continue the malware playbook.



D7 – If the malware variant is positively identified (did not have to resort to reverse engineering or behavioral analysis) download an authoritative write-up for the specific malware variant. Many antivirus/antimalware software vendor research labs publish write-ups of new malware. BleepingComputer.com also has a good collection of articles.

The information in the write-up generally includes how the malware initially infects/utilizes a dropper, operates, persists within a system, spreads to other systems, and communicates with its creator. This information gives you the power to contain, eradicate, and recover in the next step. It may also give you additional IOCs to find more infections or validate that systems are clean.

There are many sources for malware write-ups, if your favorite security tool vendor or security news hotspot doesn’t have a write up, search google or your favorite search engine for “<variant\_name> malware write up.” Be sure to compare what you collected about the malware (hashes, file names, backdoor ports, capabilities, etc.) against what the write up shows. If the write up doesn’t show the same information, it isn’t for the right variant. Keep looking.

If you perform an exhaustive search but don’t find an authoritative write up, skip this step. Not all variants have write-ups.

Document the write-up (if available) as part of your incident artifacts per your Incident Response Program requirements.

Resources:

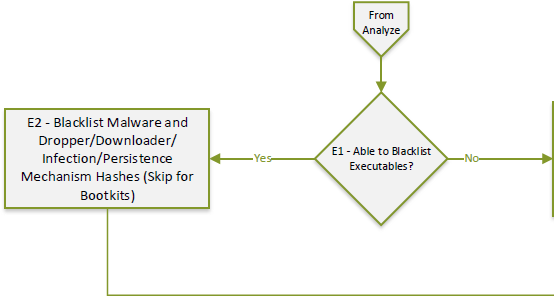
<https://blog.malwarebytes.com/category/threat-analysis/>

https://www.bleepingcomputer.com/virus-removal

<http://blog.malwaremustdie.org>

# Contain/ Eradicate/ Recover

The Contain/Eradicate/Recover phase puts all the work and information from the previous phases into action. In this phase the responders will track the malware infection back to its initial infection vector and forward through the entire infection chain until all affected systems are identified and remediated.



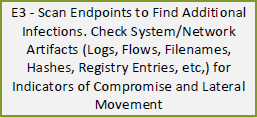
E1 & E2 – If you have the enterprise security tools available to block executables from running in your environment (generally based on file hash), add all known bad file hashes gathered in the previous phase to the blacklist in your tool. Be sure to include droppers, malware executables, and known executable support/persistence mechanisms. With most commercial tools this will stop it from executing even if it was already running.

Run a report from the tool to show which systems have the malware. Document the infected systems with your incident artifacts per your Incident Response Program requirements. You will need this information later to eradicate and recover.

If your organization does not have the capability to blacklist executables, move to E3 to use other tools to find and isolate infected hosts.

Document your tools and TTPs related to executable blacklisting and reporting here.

Document the files/hashes blacklisted as part of your incident artifacts per your Incident Response Program requirements.



E3 – This step will be highly variable based on the tools your organization has available. The ultimate goal in this step is to find any and every other infected system using the indicators of compromise gathered in the previous phase so that they can be remediated. There are a variety of tools that can accomplish this, it will be a matter of identifying the tools you have available, their capabilities for finding specific classes of IOC, and documenting them here.

The specific IOCs related to the identified malware infection used will depend upon one or more tool capabilities. Responders generally need tools that scan file systems/hashes, system and application logs, network artifacts (arp cache, dns cache, packets), registry or config files, and enumerate OS features used as persistence mechanisms (cron jobs, scheduled tasks, installed services, etc.)

Tools that can scan for IOCs (whether by automated or manual processes) include, but are not limited to:

* IOC scanners – on demand, such as Redline, Loki, or NMAP with appropriate NSEs
* IOC scanners – automated such as AMP or CounterACT
* Remote scripted searches using native OS languages/features such as bash over SSH or WMI
* Endpoint antivirus/antimalware that allows you to create custom rules
* Host based intrusion prevention software that allows you to create custom rules
* Log collection and analysis systems, such as Splunk or ELK stack, if certain OS aspects are set to log
* Network based security tools, such as Intrusion Prevention Systems or NetFlow analyzers

Each of the above toolsets has strengths in detecting some IOC’s and weaknesses in others. For instance, network based security tools are excellent at detecting communication to/from C2 internet addresses that are associated with a particular malware variant, some can even detect infected executables in a network stream. But network based security tools can’t detect whether or not a particular registry entry or cron job has been deployed to a system.

Identify gaps in your IOC detection toolset and fill them.

Document your tools and TTPs here.

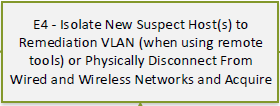
After you scan for known IOCs, add any additional infected systems to the incident and document your searches per your Incident Response Program requirements.

Resources:

<https://blogs.cisco.com/security/indicators-of-compromise-and-where-to-find-them>

<https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise>

<https://www.fireeye.com/blog/threat-research/2013/12/openioc-series-investigating-indicators-compromise-iocs.html>



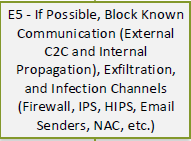
E4 – If additional endpoints exhibit indicators of compromise or are suspected to have a malware infection, isolate the new suspect hosts. If you have remote tools isolate via remediation VLAN, or disconnect the endpoint from all wireless and wired networks and remove/unplug directly attached devices. (USB storage, IoT, PLC, printers, etc.)

If the malware is capable of affecting external devices, isolate them as well.

Ideally the devices physically removed from the network should be pulled and acquired by responders to prevent ‘proactive’ users from plugging them back in. A good stakeholder communication plan as part of your incident response function and a sticky note on the device or monitor (where possible) will go a long way toward keeping potentially infected devices out of the production network until the device can be acquired or remediated.

Your organization may have tools and TTPs available to remotely help with isolation to a remediation VLAN, if so document them here.

If your organization has a specific procedure for disconnecting wireless and wired network connections and physically acquiring devices, document them here.



E5 – E5 is fed via one of two paths; from E2 where the malware executables are no longer able to run and the endpoint is still on the network, or from E4 where the endpoint has been removed from the production network (physically or via remediation vlan) and is awaiting remediation.

This step will be highly variable based on the tools your organization has available. The goal in E5 is to use any internal to internal and internal to external tools to block known communication channels used for propagation, C2 communication, and exfiltration. Communication channels can be gleaned from an authoritative write-up, reverse engineering, or direct observation of network traffic to/from infected hosts.

Possible ways to block traffic include, but are not limited to:

* Access Control lists on network firewalls or other network infrastructure
* Network Access Control (NAC) technologies
* Host-based firewalls
* Intrusion Prevention Systems (Network and host based)
* Network black-hole routes
* Proxy (Internal and remote)
* Email Filtering
* Endpoint Security Suite
* Blocks at network infrastructure via port-level (bring the interface down) or MAC address blocks.

Document actions taken to block traffic as part of your incident artifacts per your Incident Response Program requirements.

Document your tools and TTPs that can block malware traffic here.

References:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf> (Page 17)



E6 – The end goal of this step is to clean the malware files, configuration items (registry, config files, etc.), and any persistence mechanisms left behind.

An incident would not have been initiated for malware that was automatically stopped and removed by endpoint or network security tools, so it is assumed that intervention with non-standard tools is required. This may be possible through remote tools if your organization possesses the tools and the endpoint is still on the network. Otherwise, cleaning tools can be loaded on the acquired infected hosts.

If no automated cleaning tools are available (whether it is being cleaned remotely or locally), utilize information gleaned from the authoritative write-up, reverse engineering report, or from direct observation of the malware’s IOCs to remove the components of the infection.

If there is no critical information on the endpoint, or the information that is on it is deemed unrecoverable, it may make sense to re-image the workstation to save time and get it back to a known-good state. Before reimaging, pull any forensic data you will need to further investigate the malware incident.

Document the conditions where the endpoint will be re-imaged rather than cleaned here. If your organization doesn’t have guidelines, use the advice from NIST 800-83 r1:

In general, organizations should rebuild any host that has any of the following incident characteristics, instead of performing typical eradication actions (disinfection):

* One or more attackers gained administrator-level access to the host.
* Unauthorized administrator-level access to the host was available to anyone through a backdoor, an unprotected share created by a worm, or other means.
* System files were replaced by a Trojan horse, backdoor, rootkit, attacker tools, or other means.
* The host is unstable or does not function properly after the malware has been eradicated by antivirus software or other programs or techniques. This indicates that either the malware has not been eradicated completely or that it has caused damage to important system or application files or settings.
* There is doubt about the nature of and extent of the infection or any unauthorized access gained because of the infection.

If a malware incident does not have any of these characteristics, then it is typically sufficient to eradicate the malware from the host instead of rebuilding the host.

(Source: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>, page 41)

Document your tools and TTPs related to malware infection removal here. Be sure to include options for malware variants that do not have automated cleaners and options for remote and local cleanup.

Document actions taken to clean and/or reimage endpoints as part of your incident artifacts per your Incident Response Program requirements.



E7 – Now that the identified endpoints are clean, take steps to prevent re-infection. Utilize the information collected from the authoritative write-up, reverse engineering report, or from direct observation of the malware’s IOCs to close vulnerabilities, stop infected email, stop connections to infected web sites, or install new security tools to prevent re-infection of the newly cleaned devices and future infection of other devices.

Document actions taken to prevent reinfection as part of your incident artifacts per your Incident Response Program requirements.



E8 & E9 – Specific varieties of bootkits and rootkits cannot be removed by security tools without leaving the cleaned system in an unusable state. In the case of bootkits that edit the master boot record, antivirus/antimalware may corrupt the MBR, making the system un-bootable. Removal of new BIOS/UEFI infecting rootkits may not be possible without reapplying the firmware.

In these cases (there may be others) the infected endpoint should be forensically imaged and/or critical files should be saved after verifying they are not infected and the endpoint should be rebuilt from scratch to avoid the possibility of infection persistence.

For bootkits, the drive should be wiped and re-partitioned before rebuilding.

For BIOS/UEFI rootkits, the firmware must be re-flashed to NVRAM before rebuilding.

Document actions taken to clean rootkits and bootkits as part of your incident artifacts per your Incident Response Program requirements.



E10 - Utilize the information collected from the authoritative write-up, reverse engineering report, or from direct observation of the malware’s IOCs to determine whether or not the malware variant has the capability to activate a trojan horse, backdoor, reverse shell, remote access tool, or other means of giving the attacker direct access to the infected endpoint.

Even if there is no immediate evidence that remote access has occurred, initiate the System Compromise/Breach playbook in addition to this playbook to investigate the possibility in detail and respond appropriately. Both playbooks can be run in parallel if there are enough responder resources to do so.

Document additional playbooks initiated as part of your incident artifacts per your Incident Response Program requirements.

Keep in mind that recovery efforts in this playbook could hamper the investigation in the System Compromise/Breach playbook. Evaluate what actions are needed outside of this playbook prior to making changes to the infected system.

In either case, continue to E11.



E11 - Utilize the information collected from the authoritative write-up, reverse engineering report, or from direct observation of the malware’s IOCs to determine whether or not the malware variant has the capability to collect and exfiltrate sensitive data via botnet, man in the browser, keylogger, etc.

Even if there is no immediate evidence that data loss has occurred, initiate the Data Loss/Theft playbook in addition to this playbook to investigate the possibility in detail and respond appropriately. Both playbooks can be run in parallel if there are enough responder resources to do so.

Document additional playbooks initiated as part of your incident artifacts per your Incident Response Program requirements.

Keep in mind that recovery efforts in this playbook could hamper the investigation in the Data Loss/Theft playbook. Evaluate what actions are needed outside of this playbook prior to making changes to the infected system.

In either case, continue to E12.



E12 – E14 - Utilize the information collected from the authoritative write-up, reverse engineering report, or from direct observation of the malware’s IOCs to determine whether or not the malware variant has the capability to collect and exfiltrate user or system credentials via keylogger, man in the browser, etc.

Even if there is no immediate evidence that credential loss has occurred, immediately change passwords or disable accounts for sites and services that the user has accessed from the infected device.

If possible, utilize SIEM logs or system logs to determine whether or not systems have been accessed using stolen credentials. Look for unexpected source addresses trying to access external systems and unexpected login failures from one or more systems. Check the resources below for more detection and mitigation tactics.

Document actions taken to change or disable accounts and check for authority/credential misuse as part of your incident artifacts per your Incident Response Program requirements.

Document tools and TTPs related to investigating stolen credentials here.

Resources:

<https://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-216.pdf>

<https://securitytoday.com/Articles/2017/09/29/Credential-Compromise.aspx>



E15 – If signs of account compromise are detected in the previous step, initiate the Authority/Credental Misuse playbook in addition to this playbook to investigate in detail and respond appropriately. Both playbooks can be run in parallel if there are enough responder resources to do so.

Document additional playbooks initiated as part of your incident artifacts per your Incident Response Program requirements.

Keep in mind that recovery efforts in this playbook could hamper the investigation in the Authority/Credental Misuse playbook. Evaluate what actions are needed outside of this playbook prior to making changes to the infected system.

In either case, continue to E16.



E16 - To ensure responders remediate the entirety of the malware infection, employ knowledge of its infection and spreading mechanism in combination with logs/alerts/reports from security tools and forensics data to trace the malware back to its initial infection. Likewise, for spreading variants, track infected endpoint activities forward.

In both cases the goal is to make sure responders can account for all of the systems involved in the infection.

The tools and TTPs utilized will vary depending upon what tools and TTPs are deployed. In general, various logging systems and network traffic analyzers/intrusion prevention will carry the bulk of the evidence trail.

Document investigative actions taken to identify additional malware components as part of your incident artifacts per your Incident Response Program requirements.

Document tools and TTPs related to investigating and following the spread of malware here.



E17 – Utilize all of the IOCs and information about the infection chain to re-scan the entire network for IOCs and further signs of lateral movement. This scan will be similar to E3, but responders may have more IOCs to search for now.

If additional infected endpoints are found, start them over at E4.

If no additional infected endpoints are found, continue to E18.

Copy any documented tools and TTPs from E3 here. If additional tools are identified to scan additional indicators found since E3, make sure you document them in E3 as well for reference in future incidents.

After you scan for known IOCs, add any additional infected systems to the incident and document your searches per your Incident Response Program requirements.



E18 – E20 – If files were damaged beyond repair or were not able to be uninfected, it may be necessary to restore files from backup. Normally, endpoint security tools will show unrepairable files in their log. If your organization has deployed file integrity monitoring, it may also clue responders in to corrupt files.

If backups are available, restore the files from backup. If backups are not available, it is best to delete them in case they are infected and could cause re-infection.



E21– If additional communication or infection channels were identified during the investigation loop between E4 – E17, block them. This step is the same as E5.

Document tools and TTPs that can block communication channels and infection vectors here. These can be copied from E5.

Document actions taken as part of your incident artifacts per your Incident Response Program requirements.



E22 – Endpoints can now be returned and/or reconnected to the production network.

Document returned/reconnected endpoints as part of your incident artifacts per your Incident Response Program requirements.



E23 – If a security tool did not detect or alert, but should have, follow the vendor’s process to send samples, indicators, traffic captures, etc. for analysis.

Document what was sent and to whom it was sent as part of your incident artifacts per your Incident Response Program requirements.



E24 – Review all indicators and behaviors of the malware. Implement new or custom rules in your security tools to detect or prevent the variant encountered in the future. What tools are modified will highly depend on your organization’s environment.

Document tools and TTPs related to the ability to deploy custom rules in your security tools here.

Document what was added or modified to each tool as part of your incident artifacts per your Incident Response Program requirements.

# Post-Incident

The Post-Incident phase covers the assessments and activities that occur after the malware threat has been remediated. These include various reviews and reports that are sent to upper management and are stored, gap assessments and corrective actions, and additions or modifications to playbooks, internal documentation, and TTPs.



F1 - Incident Review is an event and report for stakeholders and upper management to review and provide input about what happened, when it happened, how it happened, how it was investigated, and how it was remediated.

Summarize and cover everything documented throughout the various phases and steps. Identify improvement opportunities and roadblocks.

The ultimate goals are to communicate damages the business sustained, how they will be dealt with, and what will be done different in the future to stop it from happening again. Additionally, cover any continuing actions (legal action, regulatory action, other playbooks triggered, technical or procedural improvements, etc.) and who is handling them.

Resource:

<https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf> (page 44)

<https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5BNASA%20Information%20Security%20Incident%20Management%5D.pdf> (page 21)



F2 – The Lessons Learned Review may be spliced into F1 for smaller incidents. Stakeholders and upper management is invited to review and provide input.

This event and report will cover the “what-if” scenarios.

* Could any unforeseen events during the incident been detected earlier or prevented?
* What pre-cursors did we miss?
* How can we handle this type of event better in the future?
* What would we do different next time?
* What was stopping us from making progress on the incident that we didn’t recognize at the time?

Resource:

<https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf> (page 44)



F3 – The Lessons Applied Review may be spliced into F1 for smaller incidents. Again, stakeholders and upper management is invited to review and provide input.

This event and report will cover any corrective actions that have been taken, or will soon be taken, as a result of the incident. At minimum this will include actions taken during E7. If additional/updated tools or TTPs will be deployed, they should be reported about here.



F4 – This step takes the information from F1 – F3 and puts it to use with appropriate analysts and engineers to find gaps in your organization’s security tools and TTPs. Executable corrective action plans with required budget are submitted to management.

If the incident was ruled a false-positive from Detect, this step is optional.



F5 – In this step the responders take update documentation based on information discovered during the incident and the assessments/reviews above. Internal documentation, help desk documentation, internal procedures, playbooks, network diagrams, inventories, etc. are updated and fed back into the prepare phase to be applied to other phases in this playbook and other playbooks.

If the incident was ruled a false-positive from Detect, this step is optional.

Resource:

<https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf> (page 45)

<https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5BNASA%20Information%20Security%20Incident%20Management%5D.pdf> (page 22)



F6 – In this final step before the incident is completely finished, all final reports (from above) are sent to appropriate stakeholders and upper management. Wait until the end of the process to send them as responders may find additions or changes need to be made to the reports based on the updates in F5.

If the incident was ruled a false-positive from Detect, this step is optional.

Resource:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (page 54)