**Malware Playbook**

**Scope**

This Playbook covers the steps to take when malware is detected on a system.

**1. Preparation**

**Summary**

- Create and maintain a list of

- all domains owned by Organisation.

- This can prevent you from taking actions against our own domains

- all people of can register domains

- Create email template

- to notify all employees of ongoing phishing campaign against the organization

- to contact hosting organisation for domain(s) take down

- to inform 3rd party to take actions against phishing on their infra (Microsoft, Amazon, etc.)

- Ensure that:

- Mail anti-malware/anti-spam/anti-phish solutions are in place.

- Users know how to report phish

- Detection exists for office documents spawning processes

- PowerShell

- CMD

- WMI

- MSHTA

- Etc.

- Perform dry drills to ensure all aspects of the Playbook are working

- After publication

- At least once a quarter

- Test/Validate:

- Internal Contact and Escalation Paths

- Review threat intelligence for

- threats to the organisation,

- trends for the sector,

- common patterns

- newly developing risks and vulnerabilities

- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following

- IR Playbooks to highlight information security risks faced by employees, including:

- Phishing attacks and malicious emails;

- Ransomware;

- Reporting a suspected cyber incident.

**Tool Access and Provisioning**

**Tools**

Please referrer to [DCOT Handbook]

**Assets List**

- A list of assets and owner should exist and be available for the following

- Customers Assets

- Owners

- Contacts

- Pre approved/authorized actions

- Organisation Assets

- Owners

- Contacts

- Administrators

- Pre approved/authorized actions

- Type of assets inventory needed

- Endpoints

- Servers

- Network Equipment

- Security Appliances

- Network Ranges

- Public

- Private

- VPN / Out of Band

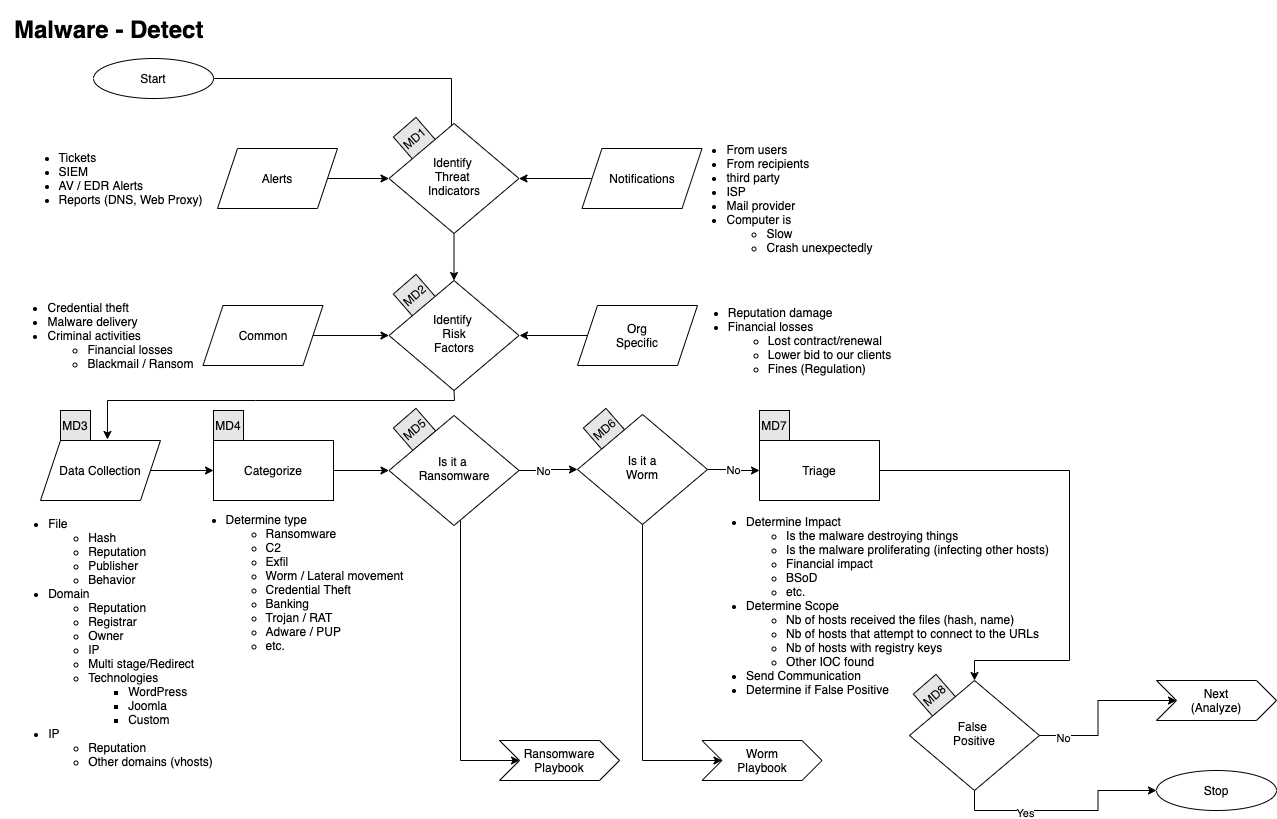
- Employees

- Partners

- Clients

**2. Detect**

**Workflow**



**Identify Threat Indicators**

**Alerts**

Alerts are be generated by different systems. The main sources for alerts are

- Tickets

- SIEM

- Anti-Virus / EDR

- Reports

- DNS

- Web Proxy

- Errors from mail servers

**Notifications**

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- Users (internal)

- Recipients of emails (external)

- Third Parties

- ISP

- Mail Providers

- Computer is

- Slow

- Crash unexpectedly

**Identify Risks Factors**

**Common**

- Credential Theft

- Malware Delivery

- Criminal Activities

- Blackmail / Ransom

**Organisation Specific**

- Reputation damage

- Financial Losses

- Lost of contract

- Contract not renewed

- Lower bid to our clients

- Fines

- Regulation

**Data Collection**

This section describes the information that should be collected and documented about the incident.

**Files**

- Hash

- Reputation

- Publisher

- Behaviour

**Domains**

- Reputation

- Registrar

- Owner

- IP

- Multistage / Redirect

- Technologies of the site

- WordPress

- Joomla

- Custom Page (credential phish)

**Intellectual Property**

- Reputation

- Owner

- Geo Localisation

- Other domains on that IP

**Categorize**

**Determine type of malware**

- Ransomware

- C2

- Exfiltration

- Worm / Lateral Movement

- Credential Theft

- Banking

- Trojan / RAT

- Adware / PUP

- etc.

**Is it a Ransomware**

As time is VERY sensitive in the case of a Ransomware:

- Send a communication to the DSOC

- Ping everyone in the DCOT Chat

- Go to the **Ransomware Playbook**

- If the Playbook doesn't exist, follow this one

**Is it a Worm**

As time is sensitive in the case of a Worm:

- Send a communication to the DSOC

- Ping everyone in the DCOT Chat

- Go to the **Worm Playbook**

- If the Playbook doesn't exist, follow this one

**Triage**

**Determine**

- Impact

- Of the malware destroying things

- Is the malware proliferating (infecting other hosts)

- Financial

- Blue Screen of Death (or other crash)

- Data loss

- etc.

- Scope: Number and list of hosts that

- Have the files

- Hash

- File name

- RegEx match (ie: INVOICE-12345.docx where `12345` is 5 random digit)

- Attempted to connect to the

- URLs

- IP

- Ports

- That have the registry keys

- Any other IOCs found

**Is it a False Positive**

If it's a False Positive:

- Document and close the incident

**If it's a True Positive**

- Send communication to

- DCOT members

- Admin Teams

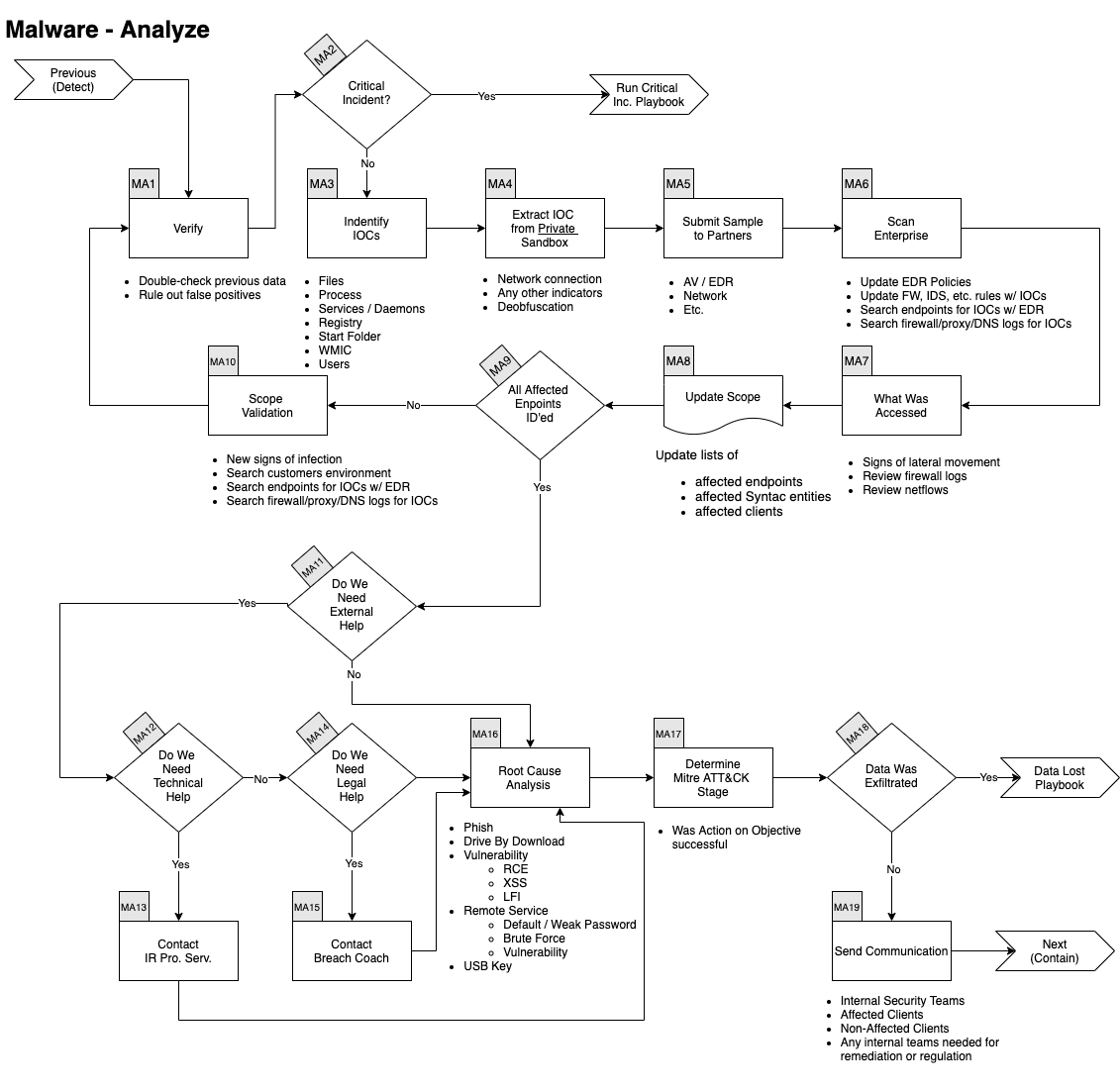
- Affected Entities

- Affected Clients

-Go to **Analyse phase**

**3. Analyse**

**Workflow**



**Verify**

In conjunction with a senior member of the DCOT

- Double check previous data

- Rule out False Positive

**Is this a Major/Critical Incident**

If this incident is deemed Major or Critical by the senior analyst go to the **Critical Incident Playbook**

**Identify IOCs**

Don't forget to look at ALL the tabs of the tools. Not just detection rate.

For example, the tabs `Details` and `Behaviour` of VirusTotal are very informative about who published the file and what the file did to the system.

- Validate hashes

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- Validate links

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- [URLScan](Tools)

- ID other addresses, domains, IPs

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- [Intelligence](Tools)

- Search Threat Intel sources

- [VirusTotal](Tools)

- [Hybrid Analysis](Tools)

- [Intelligence](Tools)

- Disk forensics on recipient's endpoint

**Extract IOCs**

Using a PRIVATE sandbox run the malware sample (files) and try to access the URLs

Collect the following information’s:

- Network connections

- Registries modifications

- Files

- dropped

- accessed

- modified

- Deobfuscated script

- From Script Block (for PowerShell)

- New services

- Created

- Launched

- New scheduled tasks

- New WMI provider(s)

**Submit Samples to Partners**

If the malware(s) was not detected/blocked by the security stack

- Submit Samples to Security Vendor

- Submit URLs, IP, Domains

**Scan Enterprise**

- Update AV / EDR

- Engine

- Ruleset

- Policies

- Update FW, IDS, etc. rules with IOCs

- Search endpoints for IOCs with EDR

- Search SIEM for IOCs

- Search Firewall, Proxy, DNS logs for IOCs

**What Was Access**

- Look for signs of lateral Movement

- Review firewall logs

- Network appliances (ie: Cisco ASA)

- endpoint (ie: Windows local firewall, EDR, AV, etc.)

- Review netflows

**Update Scope**

- Update lists of

- affected endpoints

- affected Company Entities

- affected clients

**Scope Validation**

Have all the machines been identified

If you find further traces of infection or new IOCs go back to the **Verify Step.**

When you are done identifying all compromised:

- Hosts

And investigated all:

- URLs

- Domains

- IP

- Ports

- Files

- Hash

**Do We Need External Help**

Depending on the depth and breadth of the infection we might need so counselling.

Evaluate of we need

- Technical, Hands On, Response, etc. support

- Legal counselling (data breach, lots of clients affected, etc.)

If it's the case, contact our partners and activate the retainer.

**Root Cause Analysis**

**How did this infection started**

- Phish

- Drive by download

- Vulnerability

- RCE

- XSS

- LFI

- Remote services

- Default / Weak password

- Brute Force

- Vulnerability

- USB key/drive

**Determine Mitre ATT&CK Stage**

The **Mitre ATT&CK Framework** as various Tactics that are part of a Cyber Kill Chain.

It is important to know at which stage of the Kill Chain the attack was detected and stopped.

**Document your ticket with the following information:**

- Stage of detection

- Stage of prevention

- Was action on objective completed

- File encrypted

- Data exfiltrated

- Account takeover

- Etc.

If data was exfiltrated go to the **Data Lost Playbook**.

**Was Any Data Exfiltrated**

If we know or suspect that data was exfiltrated by the adversaries go to **Data Loss Playbook**.

**Send communication**

- Send an update communication to

- Security Team

- Admin Teams

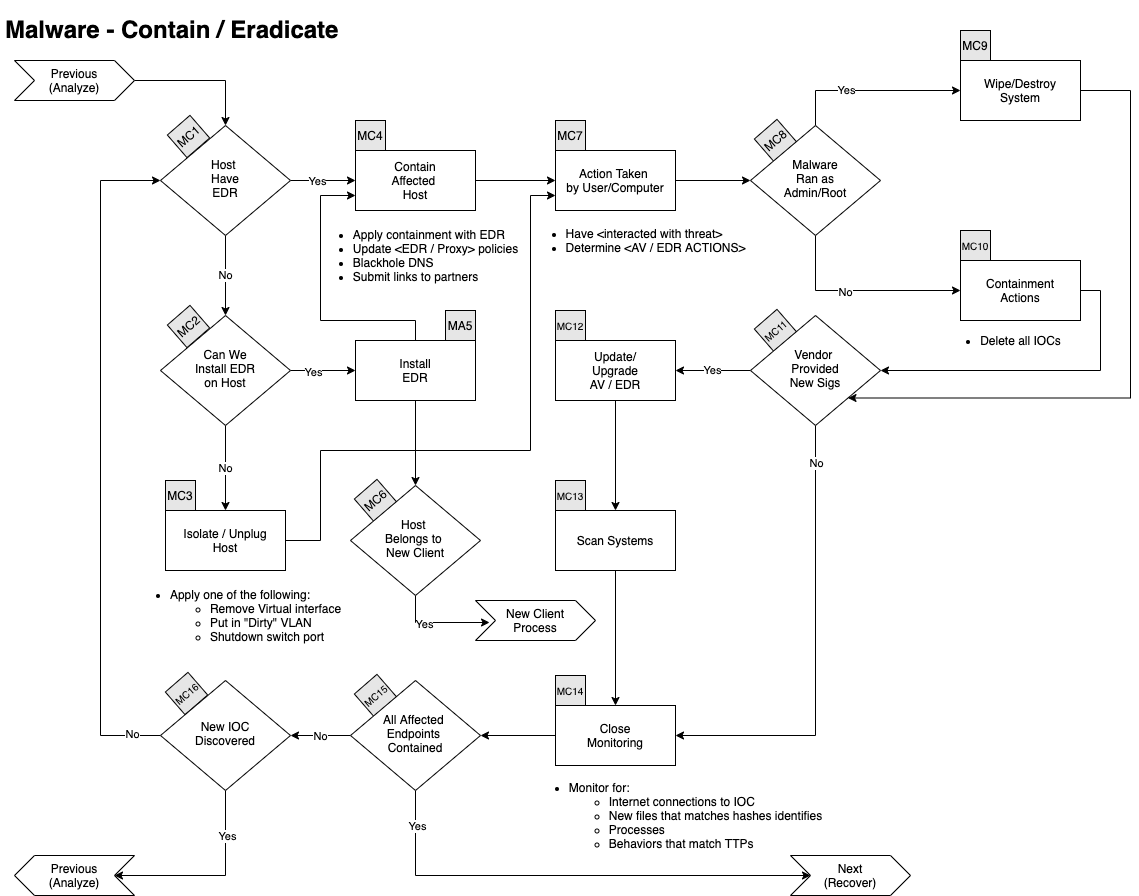
- Affected Syntac Entities

- Affected Clients

Go to the next phase **Contain/Eradicate.**

**4. Contain / Eradicate**

**Workflow**



**Does the host have EDR**

If the host have an EDR installed go to the **Contain Section**.

If the host does not have an EDR, is it possible to install one

Yes:

- Install EDR

- Go to **Contain section**

No: Isolate / Unplug the host

- Apply one of the following containment strategies

- Remove/shutdown virtual interface

- Put in "Dirty" VLAN

- Shutdown switch port

- Go to **Action Taken section**

**Contain Affected Hosts**

- Update FW, Proxy, etc. rules

- Blackhole DNS

- Submit to Partners

- AV/EDR Vendor

- Web Filter Vendor

- etc.

**Action Taken by User/Computer**

**Did the user:**

- Launch the malware

- Open the document(s)

- Run the executable

- Launch the script

**Did the computer / EDR:**

- Connect to external site(s)

- Write files to disk

- Modified registry keys

- New services

- Created

- Launched

- New scheduled tasks

- New WMI provider(s)

- Block excution

- Quarantine file(s)

**Admin Rights**

In order to select the right eradication strategy, we need to know in which context the malware was executed.

**Was the user admin/root of the machine or any other machines in the environment**

Yes:

- Wipe physical machine

- Delete virtual machine

No:

- Delete all IOCs

- Files

- Registry keys

- Services

- Scheduled Tasks

- WMI provider(s)

- etc.

**Did Vendor Release New Signature**

**Did the security vendor of the AV / EDR released a new engine, signature, policy to address the malware**

No:

- Go to **Close Monitoring**

Yes:

- Upgrade security solution

- Update signatures

- Activate policy

- Scan systems enterprise wide

- Include customers if required

**Close Monitoring**

- Monitor for:

- Internet connections to IOC

- New files that matches hashes identified

- Processes

- Behaviours that matched identified TTPs

**All Affected Endpoints Contained**

If all affected endpoints have been contained, you can go to the **Recover phase**, otherwise continue bellow.

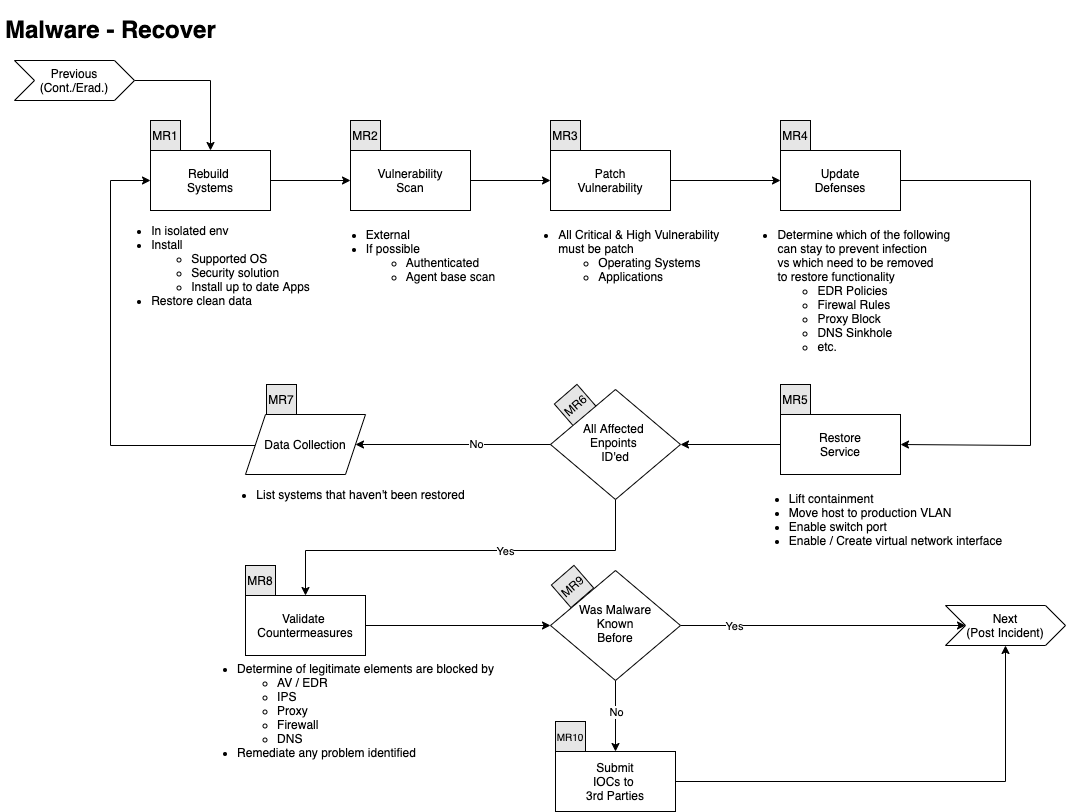
**New IOC Discovered**

If there was new IOC discovered, go back to the **Analyse Phase.**

Otherwise continue with **host containment**

**5. Recover**

**Workflow**



**Rebuilt Systems**

In an isolated environment:

- Install

- Supported OS

- Security solutions

- Up to date applications

- Restore data (from a clean backup)

**Vulnerability Scan**

Perform:

- External VA

- If possible

- Authenticated scan

- Agent base scan

**Patch Vulnerabilities**

Any Critical or High vulnerability needs to be patched before the service is re-establish.

This includes, but it not limited to

- Operating Systems

- Applications

- Network Appliances

Medium and Low vulnerability should be patched, if possible, but should not be mandatory for restoring the service/lifting containment.

**Update Defences**

Determine which of the following rules needs to be removed and which needs to stay in the following list:

- Firewall Rules

- EDR

- Ban hashes

- Ban domains

- Containment

- Proxy Block

- DNS Sinkhole

- Etc.

**Restore Service**

Depending on the containment applied to the host, perform all the following that applies:

- Lift containment in EDR console

- Move host to production VLAN

- Enable switch port

- Enable/Create virtual network interface

- etc.

**All Affected Endpoints Restored**

If all affected endpoints have been restored, you can go to the **Post Incident phase**, otherwise continue bellow.

- List systems that haven't been restored

- Go to **rebuild document**

**Validate Countermeasures**

Determine if legitimate elements are blocked by:

- AV / EDR

- IPS

- Proxy

- Firewall

- DNS

- Etc.

If so, apply the corrective action to restore functionality

**Was Malware Known Before**

If the malware was not known before the incident

- Validate with the Global Security Team if you can submit the sample to 3rd parties like

- VirusTotal

- Hybrid-Analysis

- Any.run

- Threat Grig

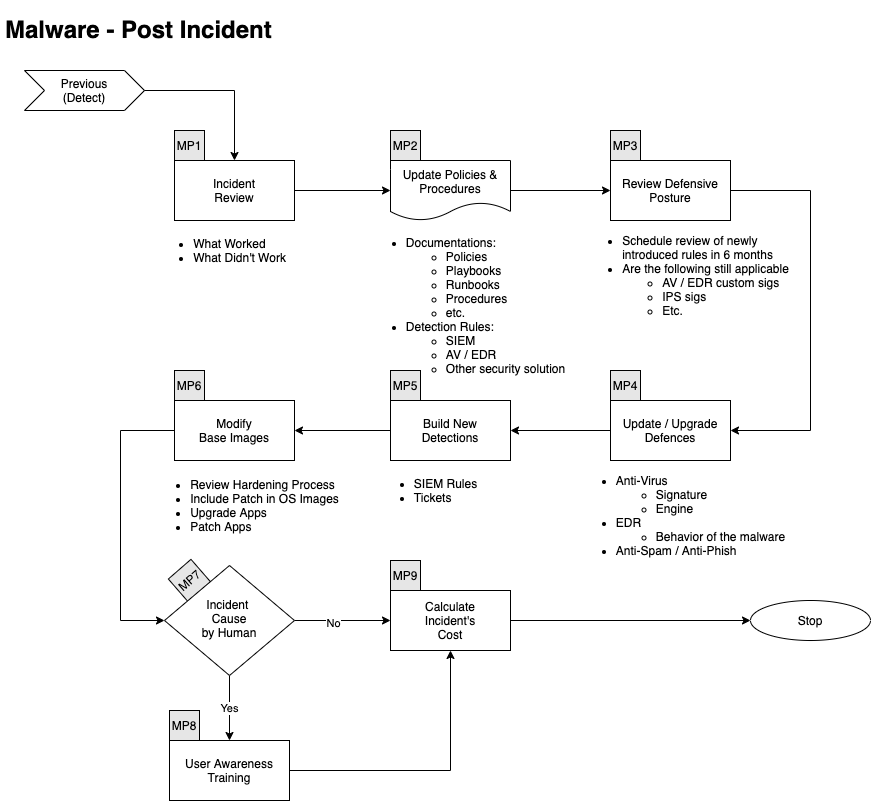
- Google Safe Browsing

- OpenIOC

- Etc.

**6. Post Incident**

**Workflow**



**Incident Review**

- What worked

- What didn't work

**Update Policies & Procedures**

Update the following documents as required:

- Policies

- Processes

- Procedures

- Playbooks

- Runbooks

Update Detection Rules in:

- SIEM

- Malware Gateway

- AV / EDR

- IPS

- Other security solution

**Review Defensive Posture**

- Schedule review of newly introduced rules in 6 months

- Are the following still applicable

- Firewall Rules

- Proxy Rules for C2

- AV / EDR custom Signatures

- IPS Signatures

- Etc.

**Update & Upgrade Defences**

As we still have multiple AV & EDR Vendor, we must ensure ALL of them can detect this malware family in the future.

Malware Sample should be sent to ALL AV and EDR vendor we work with. Once the AV/EDR vendor confirms they can detect the sample we need to make sure:

- Anti-Virus

- Signatures are updated for all

- Company Entities

- Customers (Regardless of the region)

- Engine are upgraded for all

- Company Entities

- Customers (Regardless of the region)

- EDR Rules

- To detect the behaviours of the malware

- Mail Service

- Anti-Spam / Anti-Phish

- etc.

**Build New Detections**

SIEM Rules could be created to catch this type of behaviours and create tickets.

**Modify Base Images**

If the Malware Infection was caused by a lack of hardening or insufficient patch level:

- Review hardening processes

- Include critical patches in base images

- Consider upgrading application

- Apply Security Patch to application

- etc.

**User Awareness Training**

If the incident was caused by a human error

- Create / Select new mandatory training

- From Security Education Vendor

- From YouTube video

- Built by internal teams

**Calculate Incident's Cost**

**References**

This Playbook was built using the following references:

https://www.dfir.training/index.php?option=com\_jreviews&format=ajax&url=media/download&m=14tt1&1600804844570

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf