Incident Response Playbook: Malware and Propagation Threats

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Quarterly or after major incident
Approver	SOC Manager / Head of IR

Contents

1 Introduction

1.1 Purpose

This document describes the **Malware and Propagation Threats** playbook: detection, containment, investigation, eradication and recovery guidance for malware families that propagate laterally or achieve persistence (including ransomware, commodity malware, loaders, and process/DLL injection). It is written for SOC analysts, incident responders, IT operations and leadership to provide a repeatable, operational response.

1.2 Scope

Applies to on-premise and cloud-connected endpoints, servers (Windows / Linux), file servers, Active Directory domain controllers, virtualization hosts, and cloud workloads (AWS, Azure, Office365). Includes scenarios where malware spreads via SMB/RDP, remote execution tools, compromised credentials, or fileless techniques.

2 Overview of the Category

2.1 Definition

Malware and Propagation Threats refers to malicious software or techniques that not only execute on a host but are designed to move across an environment, persist, or escalate impact. This includes: ransomware encryptors, worms, loaders (that install additional payloads), remote access trojans (RATs), exfiltration-capable trojans, and in-memory / DLL injection techniques that hide activity.

2.2 Common Attack Chain

1. **Initial Access:** phishing attachments/links, exposed RDP/SSH, vulnerable public-facing services, supply-chain compromises.
2. **Execution:** payload execution (EXE, script, macro, loader).
3. **Persistence:** services, scheduled tasks, registry autoruns, startup items, web shell.
4. **Credential Access:** credential dumping (LSASS, Mimikatz), token theft.
5. **Lateral Movement:** SMB, PsExec, WMI, RDP, SSH, remote command execution.
6. **Command & Control / Data Exfiltration:** beaconing to C2, use of cloud storage or covert channels for exfil.
7. **Impact:** encryption (ransomware), data theft, destruction or extended espionage.

2.3 Primary Risks & Business Impact

- Widespread operational outage (encrypted shared drives, unavailable services).
- Regulatory and reputational damage from data exfiltration.
- Costly recovery (forensics, rebuilds, legal/PR).
- Long-term compromise due to undetected persistence.

2.4 Common Techniques / Indicators

- Mass file modification/renaming, creation of ransom notes.
- vssadmin delete shadows or similar shadow copy deletion commands in logs.
- Unexpected service installation, scheduled tasks, or DLL loads from user directories.
- Unusual outbound DNS or HTTP(S) traffic to rare domains or Tor.
- Rapid privileged authentications across hosts (possible credential reuse).
- EDR alerts for process injection APIs (CreateRemoteThread, WriteProcessMemory).

3 Severity Level Assessment & MTTD / MTTR

Level	**Description / Criteria**	**MTTD Goal**	**MTTR Target**
Critical	Widespread encryption (ransomware) or AD/DC compromise; backups corrupted or exfil + encryption (double extortion).	$\leq$ 30 min	Containment within 4 hrs; recovery staged within 24-72 hrs
High	Multiple servers/endpoints infected with confirmed lateral movement and credential theft.	$\leq$ 1 hr	24-72 hrs
Medium	Single host infection or confirmed process injection with no confirmed lateral movement.	$\leq$ 2 hrs	12-48 hrs
Low	IOC observed, blocked by controls, no successful execution.	$\leq$ 4 hrs	Monitor (24-72 hrs)

Table 1: Severity Matrix - Malware & Propagation

4 Tools & Preparation (Recommended)

- **EDR / Endpoint Controls:** Microsoft Defender for Endpoint, CrowdStrike, SentinelOne — ensure remote isolation, live response, process tree and memory collection capability.
- **SIEM / Log Management:** Splunk, Microsoft Sentinel — centralize Sysmon, Windows Event logs, DNS, proxy, NetFlow.
- **Sysmon:** Deploy recommended Sysmon configuration (process creation, network connections, image loads).
- **Network Telemetry:** DNS logs, proxy logs, NetFlow/IPFIX, NGFW egress logging.
- **Forensics / IR Tools:** WinPMEM, FTK Imager, Volatility/Volatility3, Velociraptor for collection and triage.
- **Backups:** Immutable snapshots, air-gapped backups, documented restore playbooks.
- **Playbook Resources:** IR contact list, escalation paths, legal PR templates.

5 Incident Response Phases

(High-level steps for responding to malware propagation incidents)

5.1 Identification & Triage

Signals/Detections:

- EDR alerts showing sudden file write activity or suspicious parent-child process relationships.
- SIEM correlation: spike in file system modification events, vssadmin commands, or mass access to backup paths.
- Network: repeated DNS queries to suspicious domains or high-volume outbound uploads.

Quick actions:

- Confirm alert validity and classify severity using the Severity Matrix.
- Identify and record initial host(s) and timestamps; create incident ticket.
- Capture initial volatile evidence if safe (memory snapshot) and take EDR isolation actions as needed.

5.2 Containment (Immediate / Short-term)

- Prioritize containing lateral spread: isolate affected endpoints with EDR (network quarantine), block SMB/remote admin protocols between segments if possible.
- Block known malicious domains/IPs and update DNS sinkhole and proxy blocklists.
- Prevent backup overwrite: snapshot or disconnect backup targets; revoke write permissions from affected accounts/hosts.
- Disable compromised credentials (service accounts, scheduled tasks) to stop automated propagation.

5.3 Investigation & Forensic Triage

- Collect memory images (winpmem), process dumps, EDR full process trees, and Sysmon/Windows Event logs for affected time windows.
- Capture PCAPs for suspected C2 traffic timeframe.
- Analyze artifacts: compute hashes, YARA scanning, dynamic sandbox analysis (Hybrid-Analysis) for unknown binaries.
- Identify patient zero, lateral movement vectors and persistence mechanisms (services, scheduled tasks, registry).

5.4 Eradication

- Remove malware binaries, persistence entries, and unauthorized services/tasks after evidence capture (document all actions).
- Reimage hosts where integrity is uncertain or if persistence cannot be proven removed.
- Patch exploited vulnerabilities and harden exposed services (e.g., disable exposed RDP, enforce NLA, apply patches).
- Rotate credentials and reissue API keys and certificates that may be compromised.

5.5 Recovery

- Restore affected workloads from verified immutable backups (validate hashes prior to restore).
- Reintroduce systems to production in a staged approach with enhanced monitoring (host-based and network).
- Monitor restored systems intensively for at least 30 days for signs of re-infection.

5.6 Post-Incident Activities

- Produce full incident report, timeline, IOCs, and root-cause analysis.
- Update detection signatures (Sigma rules), YARA rules, EDR policies and SIEM correlation.
- Conduct lessons-learned session, update playbooks and run tabletop exercises.
- If applicable, coordinate notifications with Legal and Compliance for regulatory reporting.

6 MITRE ATT&CK Mapping

Malware & Propagation - ATT&CK Mapping

- **Initial Access:** T1566 (Phishing), T1078 (Valid Accounts), T1190 (Exploit Public-Facing Application)
- **Execution:** T1059 (Command and Scripting Interpreter), T1204 (User Execution)
- **Persistence:** T1543 (Create or Modify System Process), T1053 (Scheduled Task)
- **Privilege Escalation:** T1068 (Exploitation for Privilege Escalation), T1134 (Access Token Manipulation)
- **Defense Evasion:** T1027 (Obfuscated Files or Information), T1070 (Indicator Removal on Host)
- **Credential Access:** T1003 (OS Credential Dumping)
- **Lateral Movement:** T1021 (Remote Services), T1570 (Lateral Tool Transfer)
- **Command & Control:** T1071 (Application Layer Protocol), T1483 (Domain Fronting / Proxy)
- **Impact:** T1486 (Data Encrypted for Impact)

7 Key Telemetry & Logs to Collect

- **Endpoint:** EDR process trees, process command-line, loaded modules (DLLs), file creation/-modification events, registry changes.
- **Windows:** Sysmon (process create, network connect, image load), Windows Security Events (4624, 4688, 4720, 7045), Application logs.
- **Network:** DNS logs, proxy logs (HTTP/S requests), NetFlow/IPFIX, firewall egress logs, PCAPs for suspicious sessions.

- **Identity / Cloud:** IdP sign-in logs (Azure AD/Okta), VPN logs, CloudTrail/AzureActivity, Office365 audit logs.
- **Backups / Storage:** Backup job logs, snapshot metadata.

8 Subcategory Scenarios (Realistic)

Note: Each scenario below is written as an operational SOC/IR narrative — includes detection, investigative steps performed, containment actions, and final outcome.

Scenario A: Ransomware Attack — Phishing leading to lateral movement and encryption

Summary: A targeted phishing campaign delivered a weaponized Excel attachment with a macro. An employee in Finance opened the document and enabled macros. The macro executed a downloader that pulled a loader (QakBot-style) which harvested credentials and later delivered a LockBit-like encryptor to several file servers via PsExec. Shadow copies were deleted and ransom notes appeared across shares.

Detection:

- EDR alert: suspicious child process tree: `winword.exe → powershell.exe -encodedcommand → rundll32.exe (loader)`.
- SIEM: spike in file write events on file server FS01 and multiple 4663 (file access) events.
- Backup system: failed snapshot write to FS01; logs show attempted delete operations.

Investigation & Actions:

1. **Triage & classification:** Incident classified as *Critical* due to file server impact. Incident ticket opened and IR lead notified.
2. **Immediate containment:** Isolated infected workstation via EDR; suspended PsExec usage across environment by blocking the associated service account and ACLing SMB from the workstation's subnet to servers.
3. **Evidence capture:** Collected memory image from the initial host (winpmem), extracted loader binary and calculated hashes; pulled Sysmon event logs for the last 48 hours for the workstation and FS01.
4. **Hunt for lateral spread:** Searched SIEM for the loader hash and for rare process creation patterns (powershell encoded commands) across hosts. Found same loader executed on two more servers.
5. **Block C2 and prevent exfil:** Blocked observed C2 IPs at perimeter firewall and sinkholed malicious domains via internal DNS.
6. **Forensic analysis:** Dynamic analysis of loader revealed credential theft component and scheduled task that executed encryptor payload at 02:00 local time.

Containment & Eradication:

- Isolated all affected servers and took them off the network (EDR isolation) to stop encryption spread.
- Disabled compromised service account credentials and forced password rotation for admin/service accounts with possible exposure.

- Removed scheduled task artifacts and deleted malicious binaries (after collecting samples and documenting).
- Reimaged affected servers where file integrity could not be guaranteed; preserved images for forensic review.

Recovery:

- Restored FS01 and other affected systems from immutable backups (snapshots validated against known-good hashes).
- Verified restored services and monitored for re-contact to previous C2 domains for 30 days.
- Implemented additional EDR detections for loader behaviors and blocked loader file hashes across the estate.

Outcome & Lessons:

- No payment made; restoration from backups completed for critical shares within 36 hours.
- Root cause: successful macro execution; mitigations: disable macros by policy, enhance mail attachment sandboxing, and run targeted phishing campaigns for the finance team.
- Added network segmentation to limit lateral use of PsExec and restricted service account privileges.

Scenario B: Malware Infection (Non-Ransom) — Credential-stealing keylogger leading to targeted exfiltration

Summary: An employee downloaded what appeared to be a signed VPN client from a spoofed vendor site. The installer included a commodity keylogger/RAT that exfiltrated credentials and later pushed a small staged uploader that copied specific financial spreadsheets to an external cloud bucket.

Detection:

- AV/EDR: detection of a suspicious signed binary executing network connections to a rarely-seen host.
- Proxy logs: HTTP POSTs to a cloud storage endpoint from the employee's workstation outside business hours.
- DLP: alert on a rule matching sensitive financial patterns being uploaded to external cloud.

Investigation & Actions:

1. **Initial triage:** Isolated workstation and pulled EDR live response artifacts (process tree, open network sockets).
2. **Forensic collection:** Took memory capture to find injected code and credentials in memory; imaged disk for static analysis.
3. **Cloud investigation:** Queried CloudTrail / storage audit logs to enumerate the objects uploaded and source IPs; captured object metadata and timestamps.
4. **Credential mitigation:** Rotated affected user credentials and any service accounts found in memory; forced MFA re-enrollment for the user.

Containment & Eradication:

- Removed malicious binary and cleaned persistence points; aggressive hunt for other hosts with same binary/hash.
- Blocked the destination cloud host and revoked the uploader's API keys if any were used.
- Deployed YARA rule for the observed binary and pushed to EDR for estate-wide detection.

Recovery:

- Restored any modified configurations and reinstalled legitimate VPN client from verified vendor source.
- Re-reviewed access for accounts involved in the upload and notified data owners about the exfil to determine mitigation (notification/regulatory).

Outcome & Lessons:

- Exfil was limited to a subset of spreadsheets; DLP prevented larger-scale leakage.
- Tightened procurement/installation policies and introduced application whitelisting for sensitive teams.
- Improved vendor verification guidance and added automated scanning of downloaded installers in sandbox prior to deployment.

Scenario C: Suspicious DLL / Process Injection — In-memory loader using process hollowing

Summary: EDR flagged an unusual use of CreateRemoteThread / WriteProcessMemory where `notepad.exe` was used as a host for a malicious payload (process hollowing). The injected code performed credential harvesting and periodically opened an encrypted channel to a C2 domain.

Detection:

- EDR: behavior rule triggered for suspicious remote thread creation and untrusted module loaded into a trusted process.
- Sysmon: EventID 7 (ImageLoaded) showing DLL loaded from `C:.dll`.
- Network: small periodic beaconing to high-entropy domain names (DGA-like pattern) observed in DNS logs.

Investigation & Actions:

1. **Immediate action:** Suspended the affected process via EDR (preventing further execution while preserving memory image).
2. **Artifact collection:** Collected process memory dump and the DLL file for static and dynamic analysis; computed hashes and checked threat intel.
3. **Hunt:** Searched estate for presence of same DLL path/hash and similar CreateRemoteThread occurrences.
4. **Containment:** Isolated any hosts with matching indicators and blocked DNS patterns and C2 IP ranges.

Eradication:

- Removed malicious DLLs and cleaned registry/startup entries used to relaunch loader.
- Reimaged hosts where injection indicated possible rootkit-level modifications or where persistence could not be fully traced.
- Pushed EDR detection signatures for CreateRemoteThread + WriteProcessMemory sequences and image loads from user-writable locations.

Recovery & Lessons:

- Recovered hosts from trusted images and validated via hash comparisons and baseline audits.
- Enforced application control policies preventing execution of code from user-writable directories and tightened DLL load restrictions where possible.
- Increased monitoring for process hollowing API usage and added alerts for high-entropy DNS patterns.

9 Appendices

9.1 Appendix A — Useful SIEM/Investigation Queries

Splunk: find vssadmin deletions

```
index=wineventlog EventCode=4688 OR EventCode=1
| search CommandLine="vssadmin*delete*shadows"
| table _time host user CommandLine
```

Splunk: find suspicious encoded PowerShell

```
index=wineventlog EventCode=4688
| search CommandLine="-enc *" OR CommandLine="*IEX"
| table _time host user CommandLine
```

Sentinel: detect process injection patterns (example)

```
DeviceProcessEvents
| where ProcessCommandLine contains "CreateRemoteThread" or ProcessCommandLine
    contains "WriteProcessMemory"
```

9.2 Appendix B — Forensic Artifact Locations (Windows)

- Prefetch: `C:`
- Scheduled Tasks: `C:32`
- Services: registry keys under `HKLM:`
- Sysmon logs: `Microsoft-Windows-Sysmon/Operational`
- USN journal: `$Extend$UsnJrnl`

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Severity / Summary
- Affected assets and scope (hosts, shares, cloud buckets)
- Actions taken (containment, eradication, recovery)
- Root cause and recommended remediations
- IOCs (hashes, domains, IPs)
- Follow-up items and owners