CENTRE FOR
CYBERSECURITY
BELGIUM

WIPER ATTACK/RESPONSE PLAYBOOK

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
.be

EXECUTIVE SUMMARY

This playbook provides a comprehensive framework for detecting, responding to, and recovering from wiper malware attacks. Unlike ransomware, which encrypts data with the intention of receiving payment for decryption, wiper attacks are designed with a single purpose: the complete and irreversible destruction of data. This fundamental difference makes rapid detection and immediate response absolutely critical for organizational survival.

This playbook is designed for incident response teams, security operations centers (SOCs), IT administrators, and crisis management teams working in government agencies and organizations responsible for critical infrastructure.

CRITICAL SUCCESS FACTORS FOR WIPER ATTACK RESPONSE

Five critical factors determine outcomes during wiper attacks:

1. **Time is of the essence** - Detection to containment must occur as fast as possible. Wiper attacks destroy data rapidly and irreversibly.
2. **Protect Backups First**
   a. Immediately isolate backup infrastructure upon detection.
   b. Implement immutable backups as primary defense.
   c. Test restoration procedures at least once per month, Backups are your only recovery path and must be protected at all costs.
3. **Prepare Before Incidents Occur**
   a. Conduct quarterly tabletop exercises.
   b. Maintain up-to-date contact lists and procedures.
   c. Pre-establish relationships with external partners.
   d. Document and test recovery procedures.
   e. Security investments before incidents are more cost-effective by orders of magnitude than reactive measures.
4. **Coordinate Effectively**
   a. Establish clear command structure and decision authority.
   b. Implement multi-channel communication with primary and backup methods.
   c. Provide regular stakeholder updates.
   d. Coordinate with law enforcement and regulators.
   e. Share information with peer organizations.
5. **Learn and Improve Continuously**
   a. Conduct thorough post-incident reviews.
   b. Implement lessons learned.
   c. Update procedures based on new threats.
   d. Share knowledge with the community.
   e. Maintain regular training and awareness programs.

ESSENTIAL PREPAREDNESS REQUIREMENTS

Organizations must have the following capabilities in place **before** incidents occur:

- Immutable backups implemented with 30-90 days retention
- Air-gapped backups physically isolated from networks
- Periodic backup restoration testing

IMPORTANT PREPAREDNESS REQUIREMENTS

- Documented and practiced incident response plans
- 24/7 monitoring and alerting operational
- EDR deployed on all endpoints
- Network segmentation implemented
- Privileged access management in place
- Multi-factor authentication enforced
- Current security awareness training
- Verified contact lists updated regularly
- External partnerships established
- Cyber insurance policy reviewed
- Regulatory notification procedures documented
- Communication templates prepared
- Forensic tools and procedures ready

THE REALITY OF WIPER ATTACKS

Wiper attacks differ fundamentally from ransomware in their objectives and recovery options. While ransomware seeks financial gain through data encryption, wiper malware is designed to permanently destroy data. This distinction has important implications for incident response: there is no possibility of negotiation or decryption, making prevention and backup integrity the cornerstones of an effective defense strategy.

Successful protection against wiper attacks requires a multi-layered approach combining immutable backups that cannot be modified or deleted by attackers, rapid detection and response capabilities that can identify threats as quickly as possible, well-documented and regularly practiced response procedures, and systematic improvement of defenses based on emerging threats and organizational experience.

This playbook provides a structured framework for building these capabilities. Organizations that invest in comprehensive preparation, conduct regular testing of their procedures, and maintain robust backup practices that can effectively mitigate the impact of wiper attacks. The guidance contained in this document draws on real-world incident experiences and industry best practices to help organizations establish practical, achievable security postures appropriate to their risk profiles.

Table of contents

1. UNDERSTANDING WIPER ATTACKS

1.1 WHAT ARE WIPER ATTACKS?

Wiper malware represents one of the most destructive and dangerous forms of cyberattack that an organization can face. At its core, wiper malware is software specifically engineered to permanently destroy data, render systems completely inoperable, and cause maximum disruption to an organization's operations. The defining characteristic that distinguishes wiper attacks from other forms of malicious software is their single-minded focus on destruction rather than financial gain.

The nature of wiper attacks makes them particularly dangerous for several reasons. First, they leave no room for recovery through negotiation or payment. Second, wiper malware often propagates rapidly across networks using legitimate administrative tools. Third, the damage is fundamentally irreversible - data that has been overwritten cannot be recovered. Fourth, attacks are often timed strategically during holidays or weekends to maximize damage. Finally, wiper attacks typically involve multiple stages from initial compromise through coordinated destruction.

The motivations behind wiper attacks differ significantly from typical cybercrime. While ransomware operators are motivated by financial gain, wiper attacks are often launched by nation-state actors, hacktivists, or disgruntled insiders whose goal is pure disruption or retaliation.

1.2 COMMON WIPER FAMILIES

Understanding the history and characteristics of known wiper malware families provides crucial context for detection and response. Each major wiper campaign has taught the cybersecurity community important lessons about how these attacks unfold and evolve.

HISTORICAL WIPER ATTACKS

NotPetya (2017) remains the most economically devastating cyberattack in history. Disguised as ransomware, it was actually a wiper spread through a Ukrainian software supply chain compromise. It exploited EternalBlue and used legitimate tools like PsExec for lateral movement. The malware destroyed Master Boot Records, making systems unbootable with irreversible encryption.

Shamoon/Disttrack (2012, 2016, 2018) first struck Saudi Aramco in 2012, wiping 30,000 computers by overwriting disk sectors with images or corrupted data. The company's recovery required purchasing tens of thousands of new hard drives. The wiper resurfaced in 2016 and 2018 with updated variants, demonstrating sustained nation-state capabilities and strategic timing around significant regional events.

HermeticWiper (2022) was deployed against Ukrainian banks, energy companies, and IT organizations during Russia's February 2022 invasion. It abused legitimate signed drivers from EaseUS Partition Master to bypass security controls and corrupt partition tables and file systems. The attack coordinated with HermeticRansom (a decoy) and HermeticWizard (network spreader) for maximum impact.

RECENT WIPER ATTACKS (2024-2025)

PathWiper (2025) targeted Ukrainian critical infrastructure in June 2025 through compromised legitimate endpoint administration frameworks. Attackers used trusted management tools to deploy the wiper across multiple systems simultaneously. PathWiper verifies valid volumes before corrupting them, making it more reliable than earlier variants. Its use of legitimate administrative channels makes detection particularly challenging.

BlueWipe, SewerGoo, and BeepFreeze (2025) are three Iranian-linked wipers identified in late June 2025. BlueWipe and SewerGoo targeted Israeli organizations to disable storage devices on critical infrastructure. BeepFreeze attacked Albanian networks with similar destructive intent. The simultaneous development of three distinct families indicates substantial Iranian investment in destructive cyber capabilities.

No-Justice (2023-2024) was deployed by Iranian actors against Albanian parliament, telecom companies, and the national air carrier. It crashes Windows systems to prevent rebooting and used valid digital signatures to evade detection. A PowerShell script propagated the wiper across networks before coordinated activation. Attackers combined data theft with destruction in a two-phase operation.

Anubis "Wipe Mode" (2025) represents a ransomware-as-a-service group adding wiper functionality in June 2025. This mode destroys directories outright rather than encrypting for ransom. It blurs the line between financially-motivated crime and destructive attacks, making wiper capabilities accessible to broader threat actors through criminal service platforms.

1.3 ATTACK VECTORS

Wiper malware enters organizations through various attack vectors. The most common include compromised credentials and remote access, supply chain compromises (as demonstrated by NotPetya), phishing and social engineering, exploitation of unpatched vulnerabilities, and malicious insiders or compromised employee accounts. Understanding these pathways is essential for building effective defenses.

2. PRE-INCIDENT PREPARATION

2.1 ESSENTIAL PREVENTIVE MEASURES

The foundation of any effective wiper attack defense strategy rests on preparation undertaken before an incident occurs. No amount of rapid response can compensate for inadequate preparation, particularly regarding data backup and protection strategies.

BACKUP STRATEGY (CRITICAL)

Your backup strategy represents your organization's last line of defense against wiper attacks. Every organization must implement the **3-2-1-1 backup rule**: three copies of all critical data, on two different types of media, with one copy offsite, and one copy immutable or air-gapped.

The final principle is most critical for wiper protection. An immutable backup cannot be altered, encrypted, or deleted for a specified retention period, even by administrators with full privileges. An air-gapped backup is physically disconnected from your network, making it impossible for malware to reach through network connections.

Your backup strategy documentation must clearly define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems. RTO specifies maximum acceptable downtime, while RPO specifies maximum acceptable data loss measured in time.

Your backup implementation must include automated daily backups of all critical systems at minimum. Immutable backups must be configured with retention periods of at least 30 days, though 60 to 90 days is preferable. The most critical aspect is regular testing - you must conduct restoration tests at least monthly to confirm backups contain intact, uncorrupted data and can be restored within acceptable timeframes.

Reference: Cyber Fundamentals Framework at https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

NETWORK SEGMENTATION

Network segmentation creates barriers that malware must overcome to move laterally through your infrastructure. At minimum, critical systems must be separated from general user networks. Zero-trust architecture principles should guide your segmentation strategy, assuming attackers may already be present and preventing them from moving freely.

Protocols commonly abused for lateral movement including WMI, PowerShell Remoting, and RDP should be restricted to only those accounts and systems that legitimately require them. Your backup infrastructure will need to be isolated in its own network segment with extremely restricted access.

ACCESS CONTROLS

Multi-factor authentication (MFA) must be mandatory for all administrative accounts without exception. Privileged Access Management (PAM) solutions provide sophisticated controls for managing and monitoring administrative credentials through just-in-time privilege elevation, session recording, and automated credential rotation.

The principle of least privilege must be rigorously enforced. Every account should have only the minimum privileges necessary to perform its legitimate functions. Administrative accounts should be completely separate from regular user accounts, even for IT staff. Creating restricted privileged accounts for backups can also be implemented to enforce stronger backup access on monitoring, restoring or configuring them.

MONITORING INFRASTRUCTURE

Organizations should maintain either a dedicated 24/7 Security Operations Center or contract with a managed security service provider offering around-the-clock monitoring.

SIEM systems should collect and correlate log data from across your entire infrastructure. EDR solutions must be deployed on all endpoints. Network traffic analysis and centralized log aggregation with at least 90-day retention complete your monitoring foundation.

File Integrity Monitoring (FIM) provides an additional critical layer of defense against wiper attacks by continuously monitoring and detecting unauthorized changes to files and system configurations. FIM works by establishing baseline cryptographic hashes (typically SHA-256) of critical files and then continuously comparing current file states against these baselines. Any difference in hash values, file sizes, permissions, or timestamps trigger immediate alerts.

FIM is particularly effective for wiper attack detection because wipers must modify or destroy large numbers of files to achieve their objectives. By monitoring mass file modifications, unusual permission changes, and rapid changes to critical system files, FIM can detect wiper activity in its early stages before catastrophic data loss occurs. Modern FIM solutions correlate file changes with user accounts and processes responsible for the modifications, enabling rapid attribution and investigation.

Critical files and directories that should be monitored by FIM include executable and script directories, system configuration files, security logs and audit trails, credential storage locations, backup system files and configurations, database files, and any directories containing sensitive business data. When FIM detects suspicious file modification patterns such as thousands of files being modified within minutes, this serves as a high-confidence indicator of active wiper malware that requires immediate response.

2.2 CYBERFUNDAMENTALS FRAMEWORK ALIGNMENT

The Cyberfundamentals Framework provides a structured approach to implementing baseline security controls organized around five core functions:

1. Identify (understanding assets and data)
2. Protect (safeguards for critical services)
3. Detect (timely discovery of events)
4. Respond (taking action regarding incidents)
5. Recover (restoration of capabilities)

Organizations should review the comprehensive framework documentation at https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework to ensure alignment with all recommended controls.

2.3 TEAM PREPARATION

Every organization must establish a formal incident response team with clearly defined roles. The Incident Manager serves as the ultimate decision-making authority. The Technical Lead manages all technical response aspects. The Communications Lead manages all internal and external communications. A Legal/Compliance Representative provides guidance on preserving evidence and breach notification. The Business Continuity Lead focuses on maintaining essential operations. An External Partners Liaison manages relationships with third parties.

Training requirements include quarterly tabletop exercises simulating wiper attacks, annual full-scale incident response drills, regular updates on emerging threats, and technical training on forensics tools. Documentation must include up-to-date 24/7 contact lists, network diagrams, asset inventories, documented response procedures, pre-approved communication templates, and legal/regulatory notification requirements.

3. DETECTION PROTOCOLS

Early detection of wiper attacks represents the single most important factor in preventing catastrophic data loss. The faster you detect an attack in progress, the more opportunity you have to isolate affected systems and protect backup infrastructure.

3.1 INDICATORS OF COMPROMISE

Indicators of Compromise are observable artifacts or behavioral patterns that suggest a system has been breached. For wiper attacks, certain indicators warrant immediate, aggressive response.

Early Warning Signs include unusual administrative activity such as off-hours logins, mass privilege escalations, creation of new administrative accounts, disabled security tools, and modified backup configurations. Network anomalies include unexpected lateral movement, large-scale file access from single accounts, unusual outbound traffic, internal scanning, and SMB protocol abuse.

System Behavior changes include sudden spikes in disk I/O operations, mass file modifications or deletions, boot sector modifications, shadow copy deletions (particularly "vssadmin delete shadows" commands), and disabled system restore points.

File System Indicators include files replaced with random data or specific patterns, changed file extensions en masse, missing or corrupted Master Boot Records, ransom notes (which may be fake), and suspicious executables with wiper characteristics.

3.2 DETECTION TOOLS AND TECHNIQUES

SIEM ALERT RULES

Your SIEM must be configured with specific, high-fidelity alert rules categorized by severity level (see Appendix A for examples of detailed rules). **Critical alerts** indicate imminent or active wiper attacks requiring immediate incident response activation.
High priority alerts represent suspicious activities potentially indicating attack preparation or early-stage compromise.

EDR DETECTION CAPABILITIES

EDR tools provide deeper visibility through monitoring process execution chains, file system modifications at scale, registry key manipulations, network connections from unusual processes, memory injection techniques, and kernel-level modifications.

NETWORK MONITORING

Network monitoring provides visibility into communication patterns including traffic analysis for data exfiltration, protocol anomalies detection, command and control communications, and internal scanning activities.

BEHAVIORAL ANALYTICS

User and Entity Behavior Analytics supplements signature-based detection with statistical modeling of normal behavior, detecting anomalous user patterns, compromised credential usage, deviation from normal operations, and statistical anomalies in file operations.

FILE INTEGRITY MONITORING

File Integrity Monitoring (FIM) represents a critical detection layer specifically effective against wiper attacks. FIM continuously monitors files and directories for unauthorized changes by maintaining cryptographic hashes of file contents and comparing current states against known-good baselines.

For wiper attack detection, FIM provides several key capabilities. It can detect mass file modifications in real-time, alerting when large numbers of files are changed within short time periods. FIM monitors critical system files including executables, configuration files, and boot sectors for any modifications that might indicate MBR or system structure attacks. It tracks permission and ownership changes that might indicate privilege escalation or attacker preparation. Most importantly, FIM attributes all file changes to specific user accounts and processes, enabling rapid identification of compromised accounts or malicious processes.

Organizations should configure FIM to monitor critical areas including system directories (Windows System32, Program Files, /etc, /bin, /usr), configuration files (registry, system config files, application configurations), security and audit logs, credential storage locations (password vaults, key stores, certificate stores), backup system files and configurations, database directories and configuration files, and all directories containing sensitive business data.

Modern FIM solutions integrate with SIEM platforms to correlate file modification events with other security telemetry. When FIM detects a file modification event, it can be correlated with authentication logs, process execution data, and network activity to provide complete attack context. This correlation is particularly valuable for distinguishing legitimate administrative file changes from malicious wiper activity.

FIM Alert Priorities for Wiper Detection:

Critical Priority Alerts:

- Mass file modifications exceeding 100 files per minute from a single process
- Modifications to Master Boot Record or partition tables
- Changes to backup system configurations or backup files
- Shadow copy or system restore files deletion
- Modifications to security software files or configurations

High Priority Alerts:

- Unusual file permission changes affecting large numbers of files
- Modifications to system configuration files outside change windows
- Changes to log files or audit trails (potential evidence destruction)
- Rapid sequential file modifications across network shares

Implementation Considerations:

FIM solutions must be carefully tuned to reduce false positives while maintaining effective detection. Legitimate system updates, patch installations, and authorized administrative activities generate file modifications that should not trigger alerts. Organizations should establish change control procedures that integrate with FIM systems, allowing temporary suppression of alerts during approved maintenance windows.

Baseline management is critical for FIM effectiveness. Initial baselines should be established when systems are in known-good states, and baselines must be updated following legitimate changes through formal change management processes. FIM systems should maintain historical baselines enabling detection of subtle, incremental changes over extended periods.
Performance impact must be considered, particularly for systems with high file I/O activity. Modern FIM implementations use operating system-native event hooks (Windows Event Tracing for Windows, inotify/fanotify for Linux) rather than continuous polling, minimizing performance overhead while providing real-time detection.

3.3 THREAT INTELLIGENCE INTEGRATION

Intelligence sources should include CERT feeds, ISACs, commercial threat intelligence platforms, open-source intelligence, and peer organization sharing networks. Actionable intelligence includes known malware hashes, indicators of compromise from recent campaigns, tactics and techniques, associated infrastructure, and targeting information.

3.4 TRAINING RESOURCES

Detection training should include CISA training programs, MITRE ATT&CK framework training, Safe on Web AtWork Platform resources (https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework), ENISA training materials, and NCSC guidance.

4. IMMEDIATE RESPONSE PROCEDURES

When a wiper attack is detected, every second matters. Detection to containment should occur as fast as possible.

STEP 1: INITIAL DETECTION & ALERT

When a potential wiper attack is detected, first confirm the alert by looking at multiple independent indicators. Document everything including exact time, affected systems, and alert source. Activate the incident response team immediately using reliable out-of-band channels. Declare an incident level based on initial severity assessment.

Decision point: If confirmed wiper activity is detected, proceed immediately to Step 2. If uncertain but suspicious, continue monitoring while preparing for immediate containment.

STEP 2: IMMEDIATE CONTAINMENT

Speed is essential as data destruction happens rapidly. Priority actions in order:

Isolate affected systems by disconnecting network cables physically if possible, disabling WiFi adapters, and blocking at firewall level. DO NOT shut down systems as this preserves volatile memory for forensics.

Protect backup infrastructure by immediately isolating all backup systems from the network, verifying backup integrity, disabling automated backup jobs temporarily, and securing air-gapped and offsite backups.

Segment the network by implementing emergency firewall rules, blocking SMB/RDP/WMI protocols between segments, disabling domain administrative account usage, and restricting lateral movement paths.

Preserve evidence by capturing memory dumps from infected systems, collecting system logs before destruction, documenting all actions taken, and screenshotting error messages or ransom notes.

Communication should occur through out-of-band channels. Notify the **Incident Manager,** brief executive leadership, alert legal and compliance teams, but DO NOT use potentially compromised email systems.

STEP 3: ASSESSMENT & SCOPING

Determine the scope by identifying patient zero (first compromised system), this will lead to determining the initial attack vector, establishing when compromise occurred, mapping all affected systems, identifying what data has been destroyed or is at risk, and assessing whether attackers are still present in the environment.

Use SIEM correlation, EDR investigation tools, network traffic analysis, file integrity monitoring, and forensic tools for assessment. Critical questions include whether the wiper has executed or is staged, whether backups are safe and accessible, what the business impact is, and whether critical services are affected.

STEP 4: ERADICATION

Remove the threat completely from your environment. Identify all compromised systems using threat intelligence and IoCs. Scan the entire network for malware signatures and check for persistence mechanisms.
Remove attacker access by resetting ALL administrative passwords, revoking compromised credentials, disabling unauthorized accounts, and removing backdoors and persistence mechanisms.

The recommended approach is complete rebuild from **clean images** rather than cleaning infected systems. If cleaning is necessary, use updated antivirus, EDR, and specialized removal tools, but understand this is less reliable than rebuilding.

Patch vulnerabilities exploited by attackers, fix misconfigurations, and implement additional security controls **before** systems return to production.

Verification requires scanning all systems before bringing them back online, monitoring for reinfection indicators, and confirming attacker access is completely removed.

STEP 5: RECOVERY

Restore operations safely through prioritized, phased restoration.

Prioritize restoration:

- Critical infrastructure first: emergency communications, safety systems, core databases, authentication systems.
- Essential services second: financial systems, customer-facing services, communication platforms.
- Standard operations third: administrative systems, reporting, development environments. Non-critical systems last.

Restore from backups: Verify backup integrity before restoration, use the most recent clean backup (created before compromise), restore to cleaned or rebuilt systems, test functionality before full deployment, and document any data loss from the backup-to-attack gap.

Phased reconnection: Bring systems online in controlled stages, monitor each system for 24-48 hours, watch for reinfection or residual threats, and implement enhanced monitoring.

Recovery validation: Confirm data integrity, test critical business functions, verify security controls are operational, and document the recovery process and timelines.

STEP 6: POST-INCIDENT ACTIVITIES

Post-incident activities are detailed in Section 6 and include forensic analysis, lessons learned meetings, improvement actions, threat intelligence sharing, and continuous improvement cycles.

5. COORDINATION & COMMUNICATION

Effective coordination and communication are as essential to successful incident response as technical capabilities.

5.1 INTERNAL COMMUNICATION STRUCTURE

Communication methods should use phone calls as primary (not on compromised systems), personal mobile devices and SMS as backup, and avoid company email if a compromise is suspected. Use pre-established out-of-band channels like Signal or WhatsApp.

5.2 EXTERNAL COORDINATION

Mandatory notifications include regulatory bodies per specific requirements (Data Protection Authority within 72 hours for GDPR, sector-specific regulators, National CERT at https://notif.safeonweb.be), and partner organizations (MSSPs, cyber insurance immediately, critical vendors, ISACs).

The Centre for Cybersecurity Belgium (CCB) can be reached at incident@ccb.belgium.be or +32 2 501 05 60.

5.3 PUBLIC COMMUNICATION

Do not communicate publicly until executive leadership approves, legal review is complete, facts are verified, impact is understood, and regulatory notifications are made.

Communication principles include transparency (be honest about the incident), timeliness (communicate when safe to do so), accuracy (only confirmed information), empathy (acknowledge impact), and action-orientation (explain response steps).

Prepare templates in advance for internal staff alerts, external stakeholder notifications, regulatory submissions, and media statements, all reviewed by legal counsel before incidents occur.

5.4 COORDINATION TOOLS

An incident management platform should provide secure incident tracking, timeline documentation, action item assignments, and evidence collection repository.
Secure communication channels include encrypted messaging (Signal, Threema, WhatsApp), secure video conferencing, out-of-band phone systems, and physical situation rooms if needed.
Status tracking should provide regular updates every 2-4 hours during active incidents, executive dashboards, and public status pages if appropriate.

6. POST-INCIDENT ACTIVITIES

Post-incident activities transform incident response from reactive crisis management into a learning experience that strengthens security posture.

6.1 FORENSIC ANALYSIS

Comprehensive forensic analysis provides detailed understanding of the attack. Evidence preservation requires maintaining chain of custody, creating forensic images of affected systems, preserving logs and memory dumps, documenting all findings thoroughly, and securing evidence for potential legal proceedings.

Root cause analysis determines how the attack occurred and why it succeeded. Identify the initial compromise vector, map the attacker timeline, identify security control failures, analyze detection delays, and document all technical findings comprehensively.

6.2 LESSONS LEARNED MEETING

Conduct a formal lessons learned meeting within two weeks of incident resolution. Include incident response team members, IT and security leadership, business unit representatives, and external partners if involved.

Discussion topics should address what happened (factual timeline), what went well (successes to maintain), what could be improved (gaps and weaknesses), what was learned (new knowledge gained), and what will be changed (concrete actions). The deliverable should be a comprehensive lessons learned report.

6.3 IMPROVEMENT ACTIONS

Translate lessons learned into concrete improvements across three categories.

1. **Security enhancements** address technical vulnerabilities including patching identified vulnerabilities, implementing additional controls, enhancing detection capabilities, updating incident response procedures, and conducting security architecture reviews.

2. **Process improvements** address organizational weaknesses including updating response procedures, improving communication protocols, enhancing coordination mechanisms, refining escalation procedures, and updating contact lists and documentation.

3. **Training and awareness improvements** include conducting organizational debriefs, updating security awareness training, scheduling follow-up tabletop exercises, sharing anonymized findings with peers, and providing specialized training for identified gaps, conduct frequent phishing simulation exercises to strengthen the skills of employees in recognizing phishing attempts, teach users to identify and report potential social engineering techniques, such as fake customer service calls or fraudulent email requests.

6.4 THREAT INTELLIGENCE SHARING

Share information with national CERT/CTI teams, sector-specific ISACs, the Safe on Web AtWork community, law enforcement agencies, and trusted peer organizations. Share sanitized indicators of compromise, attack techniques and procedures, non-sensitive lessons learned, effective detection methods, and successful mitigation strategies.

6.5 CONTINUOUS IMPROVEMENT CYCLE

Ongoing activities should include monthly reviews of detection rules, quarterly tabletop exercises, annual full-scale incident simulations, regular backup restoration testing, continuous security control assessment, and ongoing threat landscape monitoring and adaptation.

7. APPENDICES

APPENDIX A: WIPER ATTACK INDICATORS REFERENCE

Common commands used by wipers include:

- vssadmin delete shadows /all /quiet
- wbadmin delete catalog -quiet
- bcdedit /set {default} recoveryenabled no
- bcdedit /set {default} bootstatuspolicy ignoreallfailures
- wmic shadowcopy delete
- reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
- net stop "backup service name"
- sc config "backup service name" start= disabled

File system artifacts include overwritten files with zeros or random data, missing or corrupted MBR, corrupted partition tables, deleted shadow copies, modified boot configurations, suspicious executables in temp directories, and unusual scheduled tasks.

Network indicators include connections to known C2 infrastructure, lateral movement via WMI/PsExec/SMB, unusual outbound transfers, internal reconnaissance scanning, and abnormal authentication patterns.

APPENDIX B: QUICK REFERENCE CARD FOR FIRST RESPONDERS

WIPER ATTACK - IMMEDIATE ACTIONS YOU HAVE 15-30 MINUTES TO CONTAIN

1. **ISOLATE**
   - Disconnect affected systems from network (physically)
   - DO NOT power off systems (preserve evidence)
   - Alert incident response team
2. **PROTECT BACKUPS**
   - Isolate ALL backup systems immediately
   - Verify backup infrastructure not compromised
   - Disable automated backup jobs
3. **CONTAIN**
   - Block lateral movement (SMB, RDP, WMI)
   - Segment network
   - Reset admin credentials
4. **NOTIFY**
   - Incident Manager: _______________
   - CISO: _______________
   - Executive Leadership: _______________
   - Law Enforcement: _______________
   - CCB CERT: https://notif.safeonweb.be, incident@ccb.belgium.be or +32 2 501 05 60.
5. **Emergency Contacts:**
   - Full Playbook Location: _______________
   - Emergency Hotline: _______________
   - Incident Tracker: _______________

APPENDIX C: IMMUTABLE BACKUP IMPLEMENTATION GUIDE

Immutable backups provide write-once, read-many (WORM) protection that cannot be altered or deleted even by administrators until the retention period expires.

IMPLEMENTATION OPTIONS:

Cloud-Based Immutable Storage:

- AWS S3 Object Lock: COMPLIANCE mode, 30-90 day retention, separate account.
- Azure Immutable Blob Storage: Time-based retention (locked), separate subscription.
- Google Cloud Storage: Locked retention policy, separate project.

On-Premises WORM Storage:

- Hardware options: Dell EMC Data Domain, NetApp SnapLock, IBM Spectrum Protect, Cohesity
- Configuration: Physical isolation, dedicated credentials, hardware-enforced protection, 30-90 day retention

Hybrid Approach (Recommended): 3-2-1-1 Strategy: 3 copies (production, on-premises backup, cloud backup), 2 media types (disk, cloud), 1 offsite (cloud in different region), 1 immutable (cloud or on-premises WORM)

IMPLEMENTATION STEPS:

1. **Assessment**: Inventory data, classify by criticality, calculate requirements, determine retention, assess budget, select solution
2. **Design**: Design architecture, plan connectivity, design credential isolation, plan scheduling, document procedures, define policies
3. **Implementation**: Procure services, configure storage, implement connectivity, create credentials, configure software, set up monitoring, document configuration
4. **Testing**: Perform initial backups, verify immutability, test restoration, measure times, validate alerts, conduct exercise
5. **Production**: Transition to production schedule, enable monitoring, train staff, document procedures, schedule testing, begin reporting

OPERATIONAL PROCEDURES:

- **Daily**: Verify completion, review logs, monitor capacity, check immutability, validate alerting
- **Weekly**: Review success rates, analyze trends, test spot restoration, review security logs, update documentation
- **Monthly**: Full restoration test, capacity review, security assessment, credential rotation, management reporting
- **Quarterly**: Full-scale exercise, architecture review, DR test, vendor review, policy updates

SECURITY BEST PRACTICES:

Credential Isolation: Use separate credential store (not AD), implement Hardware Security Module (HSM) for keys, require MFA, rotate quarterly, limit access to minimal personnel

Network Isolation: Use dedicated backup network, implement strict firewall rules, monitor all traffic, use TLS 1.3 encryption, limit connectivity to backup windows

Access Controls: Implement least privilege, use Role-Based Access Control (RBAC), require approval workflow, log all access, conduct regular reviews

APPENDIX D: REGULATORY COMPLIANCE CHECKLIST

GDPR Compliance (if personal data affected):

- Notify Data Protection Authority within 72 hours (contact@apd-gba.be / +32 2 274 48 00)
- Document nature, scope, and likely consequences
- Describe measures taken and proposed
- Notify affected individuals if high risk to rights/freedoms
- Maintain comprehensive breach records

NIS2 Directive Compliance (for covered entities):

- Early warning within 24 hours (significant incidents)
- Incident notification within 72 hours
- Intermediate report as requested
- Final report within 1 month
- Include impact assessment, IOCs, cross-border implications, technical details

Sector-Specific Requirements:

Financial Services: Notify National Bank of Belgium (NBB), follow DORA requirements, report to financial regulators
Healthcare: Patient safety notification, medical device incident reporting if applicable, health data breach procedures
Energy/Critical Infrastructure: Grid operator notification, critical infrastructure protection protocols, European coordination if cross-border

APPENDIX E: COMPARISON WITH RANSOMWARE RESPONSE

While wiper attacks share some similarities with ransomware, key differences require different response approaches.

Key Differences:

Aspect	**Ransomware**	**Wiper Attack**
Objective	Financial gain (ransom)	Destruction/disruption
Time Pressure	Moderate (days to weeks)	Extreme (minutes to hours)
Recovery Option	Potential decryption	Only from backups
Negotiation	Possible (not recommended)	Not applicable
Data Exfiltration	Often occurs	Less common
Attribution	Cybercriminals	Often nation-state/hacktivists
Response Speed	Important	CRITICAL
Backup Priority	Very High	ABSOLUTE
Law Enforcement	Recommended	Essential

Similar Response Elements:

- Immediate isolation and containment
- Backup protection
- Forensic evidence preservation
- Coordinated communication
- Lessons learned process

When to Use Which Playbook ?

Use Ransomware Playbook when: Ransom note present, files encrypted but intact, attacker demands payment, data potentially recoverable through decryption

Use Wiper Playbook when: No ransom demand, files being destroyed/overwritten, impossibly high ransom demands (fake ransomware), evidence of data destruction rather than encryption, geopolitical context suggests destructive intent
Reference: Ransomware Response Playbook at https://atwork.safeonweb.be/sites/default/files/2023-11/steps_to_take_in_case_of_ransomware_attack_def_e.pdf

APPENDIX F: BACKUP VERIFICATION CHECKLIST

PRE-INCIDENT BACKUP HEALTH CHECK (MONTHLY):

- Backup jobs completed successfully (check logs)
- Backup integrity verified (restore tests)
- Immutable backups protected (cannot be modified/deleted)
- Air-gapped backups physically isolated
- Offsite/cloud backups synchronized
- Backup retention policies enforced
- Backup credentials secured (separate from production)
- Backup infrastructure patched and updated
- Backup monitoring alerts functioning
- Recovery time objectives (RTO) achievable
- Recovery point objectives (RPO) being met
- Backup documentation current and accurate

POST-INCIDENT BACKUP VERIFICATION:

- Identify last known good backup (before compromise)
- Verify backup completion status
- Check backup file integrity (checksums/hashes)
- Scan backup media for malware
- Confirm backup is accessible (not corrupted/encrypted)
- Test sample file restoration
- Document gap between backup and incident (data loss window)
- Verify backup contains all critical data
- Confirm backup credentials still valid
- Ensure backup system not compromised

BACKUP RESTORATION TEST PROCEDURE:

1. Select non-production test environment
2. Restore sample dataset from backup
3. Verify data integrity and completeness
4. Test application functionality with restored data
5. Measure restoration time (validate RTO)
6. Document any issues or gaps identified
7. Update backup procedures based on findings
8. Schedule next test (quarterly minimum)

APPENDIX G: MITRE ATT&CK FRAMEWORK MAPPING

This appendix maps wiper attack phases and defensive actions to the MITRE ATT&CK framework, providing a common language for threat analysis and defense planning. Understanding these mappings enables security teams to build detection rules, conduct threat hunting, and communicate about threats using standardized terminology.

UNDERSTANDING MITRE ATT&CK

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It organizes cyber adversary behavior into tactics (the "why" of an attack) and techniques (the "how" of an attack).

WIPER ATTACK KILL CHAIN - MITRE ATT&CK MAPPING

PHASE 1: Initial Access (TA0001)

Attackers gain their first foothold in the target environment.

Common Techniques Used in Wiper Attacks:

- **T1078: Valid Accounts** - Compromised credentials are the most common initial access method for wiper attacks. PathWiper (2025) leveraged compromised administrative console access.
- **T1566: Phishing** - Spear-phishing emails deliver malware or steal credentials. Used extensively in preparatory phases before wiper deployment.
- **T1190: Exploit Public-Facing Application** - Attackers exploit vulnerabilities in internet-facing systems. NotPetya exploited EternalBlue vulnerability.
- **T1195: Supply Chain Compromise** - Compromise of trusted software or service providers. NotPetya was distributed through Ukrainian accounting software updates.

Detection Opportunities: Monitor for unusual login patterns, failed authentication attempts, connections from unexpected geographic locations, and exploitation attempts against known vulnerabilities.

PHASE 2: Execution (TA0002)
Attackers run malicious code on victim systems.

Common Techniques:

- **T1059: Command and Scripting Interpreter** - PowerShell, cmd.exe, and bash are used to execute wiper commands and scripts. No-Justice used PowerShell scripts for propagation.
- **T1053: Scheduled Task/Job** - Wipers often use scheduled tasks for timed, coordinated execution across multiple systems.
- **T1106: Native API** - Direct system API calls to achieve data destruction while evading detection.

Detection Opportunities: Monitor for suspicious command-line executions, particularly involving shadow copy deletion, boot configuration modification, and mass file operations.

PHASE 3: Persistence (TA0003)
Attackers maintain access to systems across reboots and credential changes.

Common Techniques:

- **T1543: Create or Modify System Process** - Installing malicious services for persistence.
- **T1547: Boot or Logon Autostart Execution** - Registry run keys and startup folders.
- **T1136: Create Account** - Creating new accounts for maintained access.

Detection Opportunities: Monitor for new account creation, service installations, registry modifications to autostart locations, and unauthorized scheduled tasks.

PHASE 4: Privilege Escalation (TA0004)
Attackers gain elevated permissions necessary for deploying wipers across environments.

Common Techniques:

- **T1068: Exploitation for Privilege Escalation** - Exploiting vulnerabilities to gain SYSTEM or root privileges.
- **T1078: Valid Accounts** - Using compromised administrative credentials.
- **T1134: Access Token Manipulation** - Manipulating access tokens to gain administrative privileges.

Detection Opportunities: Monitor for unusual privilege elevation, exploitation attempts, and administrative actions from accounts that typically don't perform them.

PHASE 5: Defense Evasion (TA0005)
Attackers avoid detection by security tools and analysts.

Common Techniques:

- **T1562: Impair Defenses** - Disabling antivirus, EDR, and logging. Critical indicator of imminent wiper deployment.
  - **T1562.001: Disable or Modify Tools** - Stopping security software

  - **T1562.002: Disable Windows Event Logging** - Stopping event logging services
- **T1070: Indicator Removal** - Deleting logs and other evidence. HermeticWiper and IsaacWiper deleted logs after destruction.
  - **T1070.001: Clear Windows Event Logs** - Clearing security, system, and application logs
- **T1036: Masquerading** - Malware disguised as legitimate software. No-Justice used valid digital signatures.
- **T1553: Subvert Trust Controls** - Abusing code signing and driver signing. HermeticWiper abused legitimate EaseUS drivers.

Detection Opportunities: Alert immediately on disabled security tools, log deletion attempts, unusual driver installations, and legitimate tools used in abnormal contexts.

PHASE 6: Credential Access (TA0006)
Attackers steal credentials to expand access and enable lateral movement.

Common Techniques:

- **T1003: OS Credential Dumping** - Extracting credentials from LSASS, SAM, or other credential stores.
  - **T1003.001: LSASS Memory** - Dumping credentials from Local Security Authority Subsystem Service
- **T1555: Credentials from Password Stores** - Extracting stored credentials from browsers or password managers.

Detection Opportunities: Monitor for LSASS access by unusual processes, unauthorized access to credential stores, and use of credential dumping tools like Mimikatz.

PHASE 7: Discovery (TA0007)
Attackers map the environment to identify targets for destruction.

Common Techniques:

- **T1083: File and Directory Discovery** - Mapping file systems to identify valuable data.
- **T1082: System Information Discovery** - Gathering system configuration information.
- **T1135: Network Share Discovery** - Identifying network shares for destruction.
- **T1018: Remote System Discovery** - Identifying other systems in the network.
- **T1016: System Network Configuration Discovery** - Mapping network topology.

Detection Opportunities: Monitor for unusual file system enumeration, network scanning, and system information gathering from accounts or systems that typically don't perform these activities.

PHASE 8: Lateral Movement (TA0008)
Attackers spread across the network to maximize impact.

Common Techniques:

- **T1021: Remote Services** - Using legitimate remote access protocols for malware distribution.
  - **T1021.001: Remote Desktop Protocol** - RDP for accessing remote systems
  - **T1021.002: SMB/Windows Admin Shares** - NotPetya and Shamoon propagated via SMB
  - **T1021.006: Windows Remote Management** - WinRM and WMI for remote execution
- **T1570: Lateral Tool Transfer** - Moving wiper malware to additional systems.
- **T1080: Taint Shared Content** - Placing malware on network shares for execution by other systems.

Detection Opportunities: Monitor for unusual SMB traffic, RDP connections between systems that don't typically communicate, WMI command execution, and file transfers to multiple systems.

PHASE 9: Collection (TA0009)
Some sophisticated wiper attacks collect data before destruction for additional leverage or intelligence.

Common Techniques:

- **T1005: Data from Local System** - Gathering data from local drives before destruction.

- **T1039: Data from Network Shared Drive** - Collecting data from network shares.
- **T1074: Data Staged** - Aggregating collected data for exfiltration.

Detection Opportunities: Monitor for unusual data access patterns, large file movements, and data staging activities.

PHASE 10: Impact (TA0040) - PRIMARY WIPER OBJECTIVE
The final phase where attackers execute the destructive payload.

Primary Wiper Techniques:

- **T1561: Disk Wipe** - The core wiper functionality for destroying data.
  - **T1561.001: Disk Content Wipe** - Overwriting disk contents with random data or specific patterns. Used by Shamoon, PathWiper, and most other wipers.
  - **T1561.002: Disk Structure Wipe** - Destroying MBR, partition tables, or file system structures. Used by NotPetya, HermeticWiper, WhisperGate.

- **T1485: Data Destruction** - Destroying specific files or databases rather than entire disks. Used when targeted destruction is preferred over wholesale wiping.

- **T1490: Inhibit System Recovery** - Destroying backup and recovery capabilities to prevent recovery.
  - Deleting volume shadow copies (vssadmin delete shadows)
  - Deleting backup catalogs (wbadmin delete catalog)
  - Disabling Windows recovery (bcdedit commands)
  - Destroying backup files and systems
- **T1529: System Shutdown/Reboot** - Forcing system shutdown or reboot to complete destruction or prevent recovery efforts.

Detection Opportunities: Alert immediately on shadow copy deletion, boot configuration changes, backup system access, mass file modifications, and MBR modifications.

MITRE ATT&CK MAPPING FOR DEFENSIVE ACTIONS

This section maps defensive actions from this playbook to how they disrupt specific MITRE ATT&CK techniques.

Detection and Monitoring (Section 3)

Detection Capabilities Mapped to ATT&CK:

SIEM Alert Rules:

- Shadow copy deletion detection → Disrupts T1490 (Inhibit System Recovery)
- Mass file modification alerts → Disrupts T1561.001 (Disk Content Wipe)
- Disabled security tools → Disrupts T1562 (Impair Defenses)
- Lateral movement detection → Disrupts T1021 (Remote Services)

EDR Capabilities:

- Process execution chain monitoring → Disrupts T1059 (Command and Scripting Interpreter)
- Memory injection detection → Disrupts T1055 (Process Injection)
- Credential access monitoring → Disrupts T1003 (OS Credential Dumping)

Network Monitoring:

- SMB traffic analysis → Disrupts T1021.002 (SMB/Windows Admin Shares)
- Command and control detection → Disrupts T1071 (Application Layer Protocol)
- Reconnaissance detection → Disrupts T1018 (Remote System Discovery)

Immediate Response Procedures (Section 4)

Response Actions Mapped to ATT&CK Disruption:

Step 2 - Immediate Containment:

- Network isolation → Disrupts T1021 (Remote Services) and T1071 (Application Layer Protocol)
- Backup protection → Prevents T1490 (Inhibit System Recovery)
- Network segmentation → Disrupts T1080 (Taint Shared Content) and T1570 (Lateral Tool Transfer)
- Credential resets → Disrupts T1078 (Valid Accounts)

Step 4 - Eradication:

- Password resets → Eliminates T1078 (Valid Accounts) persistence
- Backdoor removal → Eliminates T1543 (Create or Modify System Process)
- Vulnerability patching → Prevents T1068 (Exploitation for Privilege Escalation) and T1190 (Exploit Public-Facing Application)

Pre-Incident Preparation (Section 2)

Preventive Measures Mapped to ATT&CK Mitigation:

Backup Strategy:

- Immutable backups → Mitigates T1490 (Inhibit System Recovery) and T1561 (Disk Wipe)
- Air-gapped backups → Prevents T1021 (Remote Services) from reaching backups

Network Segmentation:

- Zero-trust architecture → Mitigates T1078 (Valid Accounts) and T1021 (Remote Services)
- Lateral movement restrictions → Mitigates T1570 (Lateral Tool Transfer)

Access Controls:

- Multi-factor authentication → Mitigates T1078 (Valid Accounts)
- Privileged Access Management → Mitigates T1003 (OS Credential Dumping) and T1134 (Access Token Manipulation)
- Least privilege → Limits impact of T1068 (Exploitation for Privilege Escalation)

Monitoring Infrastructure:

- 24/7 SOC → Enables detection of all ATT&CK techniques
- EDR deployment → Detects T1055 (Process Injection), T1059 (Command and Scripting), T1562 (Impair Defenses)
- SIEM correlation → Detects complex attack chains across multiple techniques

MITRE ATT&CK Resources
For detailed information about specific techniques and sub-techniques:

- **MITRE ATT&CK Website:** https://attack.mitre.org
- **ATT&CK Navigator:** Interactive tool for visualizing technique coverage
- **Wiper-Specific Techniques:** Search for "wiper" or "disk wipe" on the ATT&CK website
- **Shamoon Entry:** https://attack.mitre.org/software/S0140/
- **Disk Wipe Technique:** https://attack.mitre.org/techniques/T1561/

Security teams should regularly review the MITRE ATT&CK framework as it is continuously updated with new techniques observed in real-world attacks.

APPENDIX H: GLOSSARY OF TERMS

Air-Gap: Physical isolation of systems from networks, preventing remote access and malware propagation.

Backdoor: Unauthorized method of bypassing normal authentication to gain access to a system.

Business Continuity Plan (BCP): Documented procedures for maintaining operations during and after a disruptive incident.

Chain of Custody: Chronological documentation of evidence handling to maintain integrity for legal proceedings.

Command and Control (C2/C&C): Infrastructure used by attackers to communicate with and control compromised systems.

Data Destruction: Intentional and irreversible deletion or corruption of data.

Disaster Recovery Plan (DRP): Documented procedures for recovering IT systems and data after a catastrophic event.

Endpoint Detection and Response (EDR): Security solution providing continuous monitoring and response capabilities for endpoints.

File Integrity Monitoring (FIM): Security technology that continuously monitors and detects unauthorized changes to files and system configurations by comparing current file states against cryptographic hash baselines. Particularly effective for detecting wiper attacks through identification of mass file modifications.

Forensics: Scientific investigation and analysis of digital evidence related to security incidents.

Hardware Security Module (HSM): A physical device that protects and manages cryptographic keys.

Immutable Backup: Backup that cannot be altered, encrypted, or deleted for a specified retention period.

Incident Response (IR): Organized approach to addressing and managing security incidents.

Indicators of Compromise (IOCs): Evidence that a system has been breached or infected.

Information Sharing and Analysis Center (ISACS): Member-driven, sector-specific organizations that provide a trusted environment for members to share timely and contextualized information about cyber threats, vulnerabilities, and incidents to collectively improve their sector's cybersecurity defenses.

Lateral Movement: Techniques used by attackers to move through a network after initial compromise.

Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to systems.

Master Boot Record (MBR): Critical boot sector of a storage device that can be targeted by wiper malware.

Managed Security Service Provider (MSSP): a third-party company that offers outsourced cybersecurity services, including security monitoring, threat detection, incident response, and compliance management.

Persistence: Techniques used to maintain access to systems across reboots and credential changes.

Privileged Access Management (PAM): Solutions for controlling and monitoring privileged account usage.

Recovery Point Objective (RPO): Maximum acceptable amount of data loss measured in time.

Recovery Time Objective (RTO): Maximum acceptable length of time to restore a function after an incident.

Ransomware: Malware that encrypts data and demands payment for decryption (distinct from wipers).

Security Information and Event Management (SIEM): Platform that aggregates and analyzes security logs and events.

Shadow Copy: Windows backup feature that creates snapshots of files or volumes (often targeted by attackers).

Threat Intelligence: Information about threats used to inform security decisions and incident response.

Traffic Light Protocol (TLP): Standard for sharing sensitive information with appropriate controls.

Wiper Malware: Destructive malware designed to permanently delete or corrupt data without ransom demands.

Write-Once Read-Many (WORM): Storage that allows data to be written once but prevents modification or deletion.

Zero Trust: Security model that requires verification of every access request regardless of source.