Ransomware Attack Response Playbook

Complete Incident Response Guide

Version 2.0
Security Operations Center

December 24, 2025

CONFIDENTIAL

Security Classification: RESTRICTED

This document contains sensitive security information.
Unauthorized disclosure is prohibited.
Handle according to organizational security policies.

Contents

List of Figures

List of Tables

Chapter 1

Executive Summary

1.1 Document Purpose

This playbook provides comprehensive guidance for detecting, responding to, and recovering from ransomware attacks. It serves as the primary reference for the Security Operations Center (SOC) and Incident Response Team (IRT) when dealing with ransomware incidents.

1.2 Scope and Applicability

- **Primary Audience:** SOC analysts, incident responders, system administrators
- **Systems Covered:** All organizational IT assets including servers, workstations, and cloud infrastructure
- **Attack Vectors:** Email phishing, drive-by downloads, RDP exploitation, supply chain attacks
- **Response Time:** Critical - requires immediate action upon detection

1.3 Key Objectives

1. Rapid detection and containment of ransomware
2. Minimize business impact and data loss
3. Preserve forensic evidence
4. Coordinate response efforts
5. Enable swift recovery operations
6. Document lessons learned

Chapter 2

Ransomware Attack Overview

2.1 Definition and Characteristics

Ransomware is a type of malicious software designed to encrypt files and demand payment for the decryption key. Modern ransomware attacks often involve:

- **Double Extortion:** Threatening to leak stolen data if ransom isn't paid
- **Triple Extortion:** Additional DDoS attacks or targeting customers/partners
- **Ransomware-as-a-Service (RaaS):** Affiliate programs enabling widespread attacks
- **Living-off-the-Land:** Using legitimate tools to evade detection

2.2 Common Ransomware Families

Table 2.1: Major Ransomware Families and Characteristics

Family	Encryption Method	Initial Vector	Notable Features
Conti	AES-256 + RSA-4096	Phishing, RDP	Fast encryption, data exfiltration
REvil	Salsa20 + RSA	RaaS, exploits	Auction site for stolen data
LockBit	AES + RSA	RaaS, insider threats	Self-spreading capability
BlackCat	AES + RSA	RaaS, compromised credentials	Written in Rust, cross-platform
Ryuk	AES-256 + RSA-2048	TrickBot, BazarLoader	Targets large organizations

2.3 Attack Lifecycle

2.3.1 Initial Access

Attackers gain entry through various methods:

1. **Phishing emails** with malicious attachments or links
2. **Exploit kits** targeting browser vulnerabilities
3. **RDP brute force** or credential stuffing
4. **Supply chain compromise** through third-party software
5. **USB devices** with autorun malware

2.3.2 Persistence and Privilege Escalation

Once inside, attackers establish persistence:

- Create backdoor accounts
- Modify registry keys
- Install rootkits
- Exploit local vulnerabilities for admin access
- Use stolen credentials

2.3.3 Lateral Movement

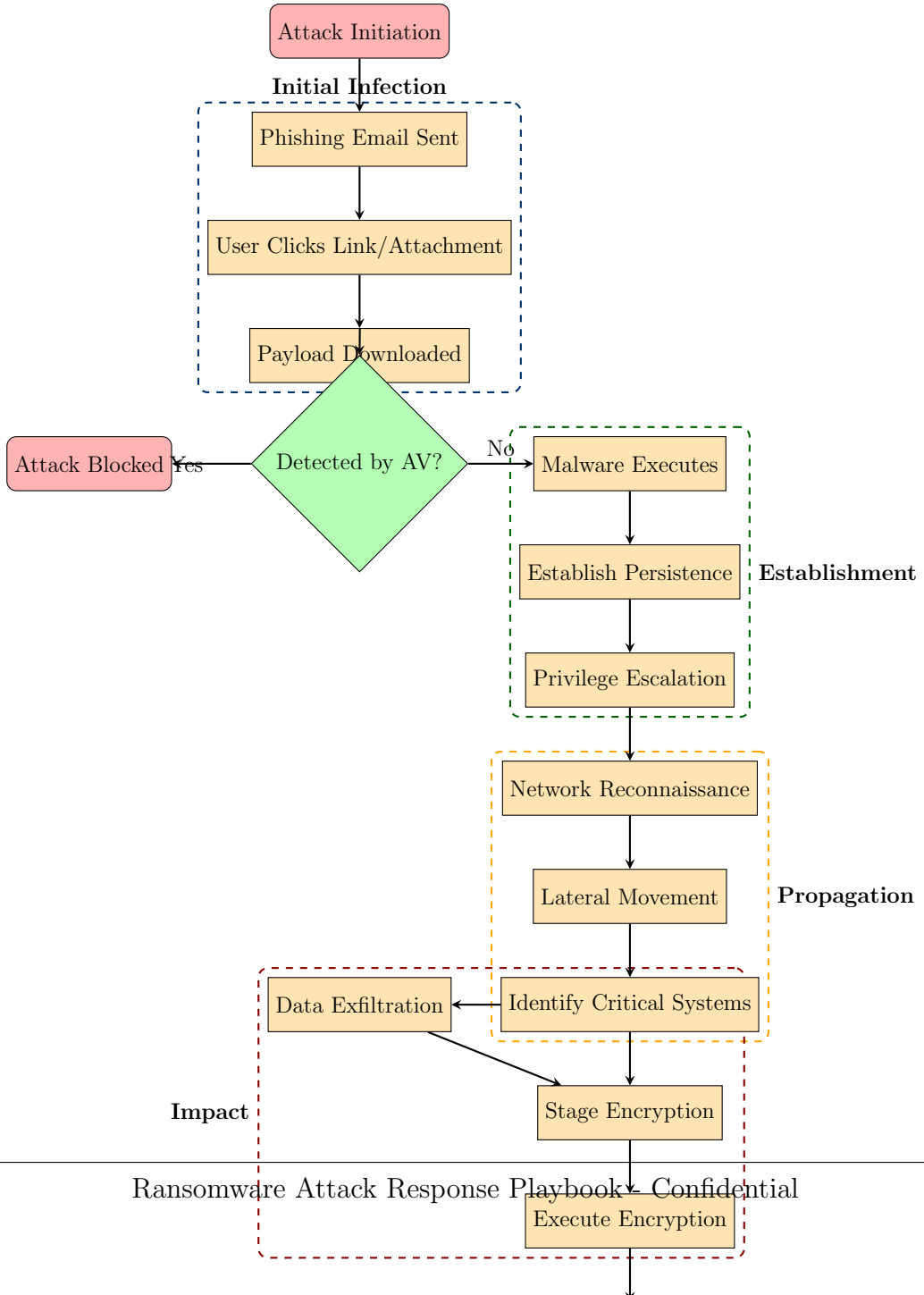
Spreading across the network:

- SMB protocol exploitation
- PsExec and similar tools
- WMI (Windows Management Instrumentation)
- RDP hopping
- Pass-the-hash attacks

Chapter 3

Attack Flow Diagram

3.1 Complete Attack Chain Flowchart



Chapter 4

Detection Mechanisms

4.1 Technical Indicators

4.1.1 Network-Based Indicators

- Unusual outbound traffic to C2 servers
- Large data transfers to unknown destinations
- TOR network connections
- DNS queries to known malicious domains
- SMB traffic anomalies
- Spike in failed authentication attempts

4.1.2 Host-Based Indicators

- Rapid file system changes
- Mass file renaming with suspicious extensions
- Shadow copy deletion
- Registry modifications
- New scheduled tasks
- Unusual process creation chains
- Memory injection activities

4.2 Detection Tools Configuration

4.2.1 SIEM Rules

```
index=windows EventCode=4663
| stats count by ComputerName, TargetFilename
| where count > 100
| eval file_extension=substr(TargetFilename, len(TargetFilename)
   -4)
| search file_extension IN (".locked", ".enc", ".encrypted", ".
   crypto")
| alert name="Potential Ransomware Activity Detected"
```

Listing 4.1: Splunk Detection Rule for Ransomware

4.2.2 EDR Detection

```
event_simpleName=ProcessRollup2
| ImageFileName=/\\vssadmin\.exe/i
| CommandLine=/delete shadows/i
| table ComputerName, UserName, CommandLine, Timestamp
| sort -Timestamp
```

Listing 4.2: CrowdStrike Falcon Query

4.3 Behavioral Analysis

Table 4.1: Behavioral Patterns and Detection Methods

Behavior	Detection Method	Tool
File encryption in bulk	File system monitoring	FSRM, Tripwire
Process injection	Memory analysis	Volatility, WinDBG
Lateral movement	Network traffic analysis	Zeek, NetworkMiner
Data exfiltration	DLP alerts	Symantec DLP, Forcepoint
Persistence mechanisms	Registry monitoring	Sysmon, Autoruns

Chapter 5

Response Procedures

5.1 Immediate Response Flowchart

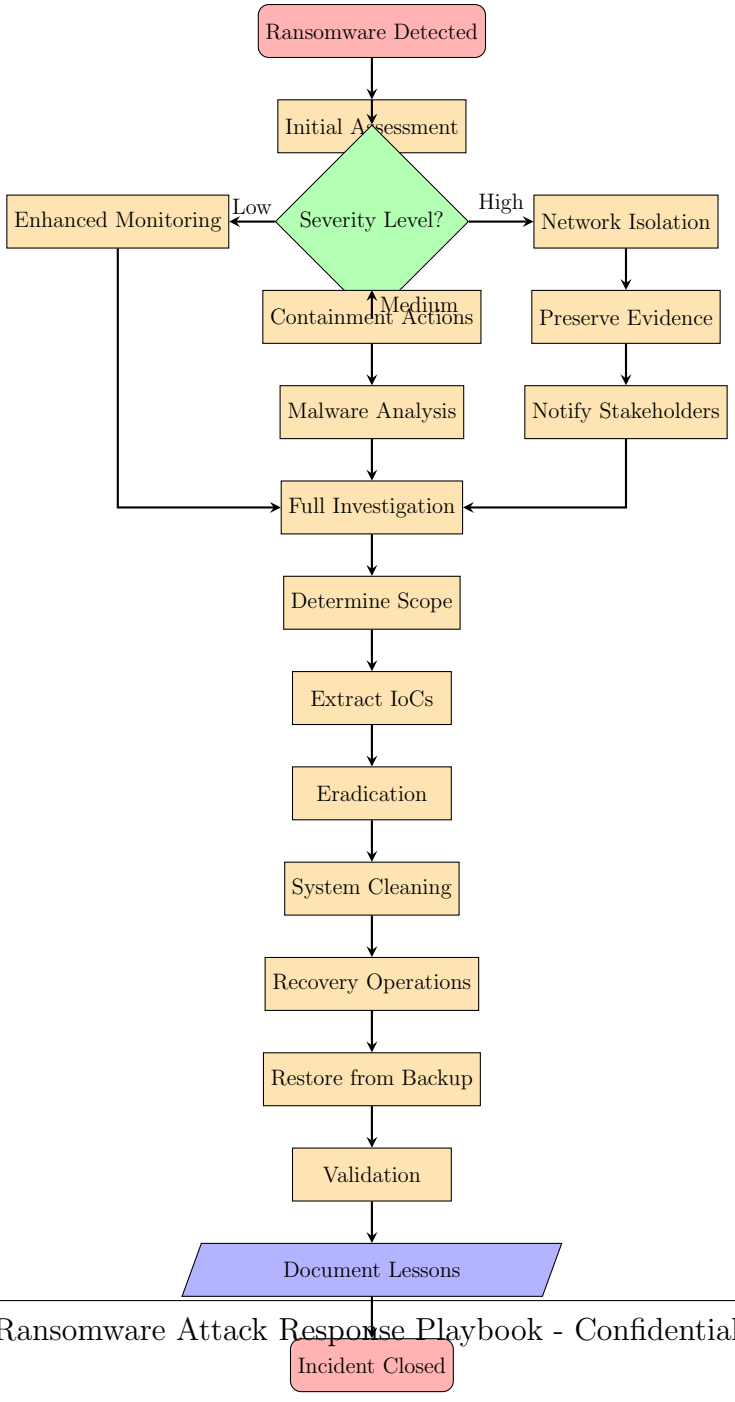


Figure 5.1: Incident Response Workflow

5.2 Containment Strategies

5.2.1 Network Isolation

1. **Immediate Actions:**
   - Disconnect affected systems from network
   - Block C2 communications at firewall
   - Disable remote access services
   - Implement network segmentation
2. **Firewall Rules:**

```
# Block known ransomware C2 domains
set security policies from any to any application any
    source any destination [malicious-ip-list]
    action deny log-end yes

# Block TOR exit nodes
set external-list tor-exit-nodes type ip
    url https://check.torproject.org/exit-addresses
set security policies block-tor source any
    destination tor-exit-nodes action deny
```

Listing 5.1: Palo Alto Firewall Blocking Rules

5.2.2 Host Isolation

```
# Disable network adapters
Get-NetAdapter | Disable-NetAdapter -Confirm:$false

# Stop suspicious services
$suspiciousServices = @("malicious_service", "unknown_svc")
foreach ($service in $suspiciousServices) {
    Stop-Service -Name $service -Force
    Set-Service -Name $service -StartupType Disabled
}

# Kill suspicious processes
$suspiciousProcesses = Get-Process | Where-Object {
    $_.Path -like "*temp*" -or
    $_.Path -like "*appdata*"
}
foreach ($proc in $suspiciousProcesses) {
    Stop-Process -Id $proc.Id -Force
}
```

Listing 5.2: PowerShell Host Isolation Script

5.3 Evidence Collection

5.3.1 Memory Forensics

```
# Windows memory dump using DumpIt
DumpIt.exe /quiet /output C:\Evidence\memory.dmp

# Linux memory dump using LiME
insmod lime.ko "path=/evidence/memory.lime format=lime"

# Analyze with Volatility
volatility -f memory.dmp imageinfo
volatility -f memory.dmp --profile=Win10x64 pslist
volatility -f memory.dmp --profile=Win10x64 netscan
```

Listing 5.3: Memory Dump Collection

5.3.2 Disk Forensics

- Create forensic images of affected systems
- Preserve file system metadata
- Document encryption patterns
- Collect ransom notes and malware samples

Chapter 6

Prevention and Mitigation

6.1 Preventive Controls

6.1.1 Technical Controls Matrix

Control Category	Implementation	Tools/Technologies
Access Control	Multi-factor authentication	Azure MFA, Duo Security
	Privileged access management	CyberArk, BeyondTrust
	Least privilege principle	Active Directory, RBAC
Endpoint Protection	Next-gen antivirus	CrowdStrike, SentinelOne
	Application whitelisting	AppLocker, Bit9
	Host-based firewall	Windows Defender Firewall
	Patch management	WSUS, SCCM, Automox
Network Security	Network segmentation	VLANs, micro-segmentation
	IDS/IPS deployment	Snort, Suricata
	DNS filtering	Cisco Umbrella, Infoblox
Data Protection	Regular backups	Veeam, Commvault
	Backup testing	Automated restoration tests
	Offline backup storage	Air-gapped systems, tapes
Email Security	Spam filtering	Proofpoint, Mimecast
	Attachment sandboxing	FireEye, Cuckoo Sandbox
	User awareness training	KnowBe4, SANS

Table 6.1: Comprehensive Prevention Controls

6.2 Backup Strategy

6.2.1 3-2-1 Backup Rule Implementation

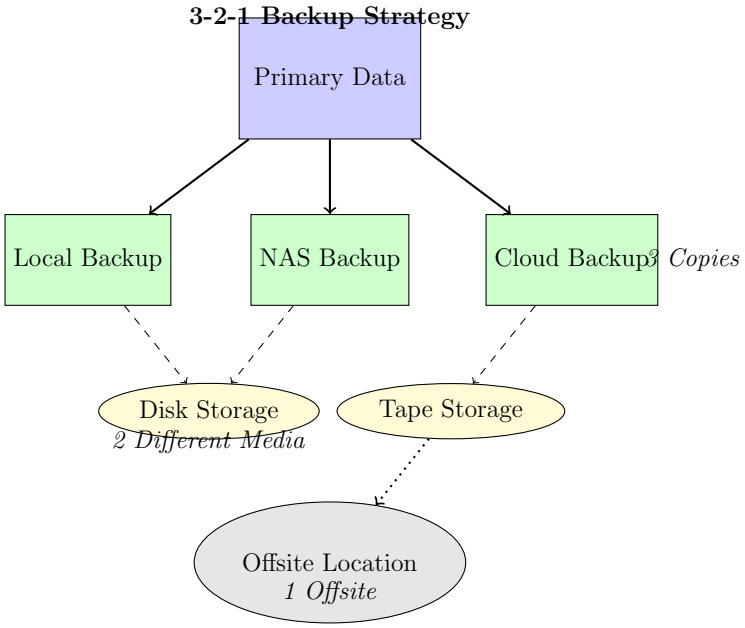


Figure 6.1: 3-2-1 Backup Strategy Visualization

6.3 Security Hardening

6.3.1 Windows Hardening Script

```
# Disable unnecessary services
$services = @('RemoteRegistry', 'TlntSvr', 'SNMP')
foreach ($svc in $services) {
    Set-Service -Name $svc -StartupType Disabled
    Stop-Service -Name $svc -Force -ErrorAction SilentlyContinue
}

# Configure Windows Defender
Set-MpPreference -DisableRealtimeMonitoring $false
Set-MpPreference -DisableBehaviorMonitoring $false
Set-MpPreference -DisableBlockAtFirstSeen $false
Set-MpPreference -DisableIOAVProtection $false
Set-MpPreference -CloudBlockLevel High
Set-MpPreference -CloudExtendedTimeout 50
Set-MpPreference -EnableControlledFolderAccess Enabled

# Disable PowerShell v2
Disable-WindowsOptionalFeature -Online -FeatureName
   MicrosoftWindowsPowerShellV2

# Enable AppLocker
```

```
Set-Service -Name AppIDSvc -StartupType Automatic
Start-Service -Name AppIDSvc

# Configure audit policies
auditpol /set /category:"Logon/Logoff" /success:enable /failure:
    enable
auditpol /set /category:"Object Access" /success:enable /failure:
    enable
auditpol /set /category:"Process Tracking" /success:enable

# Restrict administrative shares
reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\
    Parameters" /v AutoShareWks /t REG_DWORD /d 0 /f
```

Listing 6.1: PowerShell Hardening Script

Chapter 7

Recovery Procedures

7.1 Recovery Decision Tree

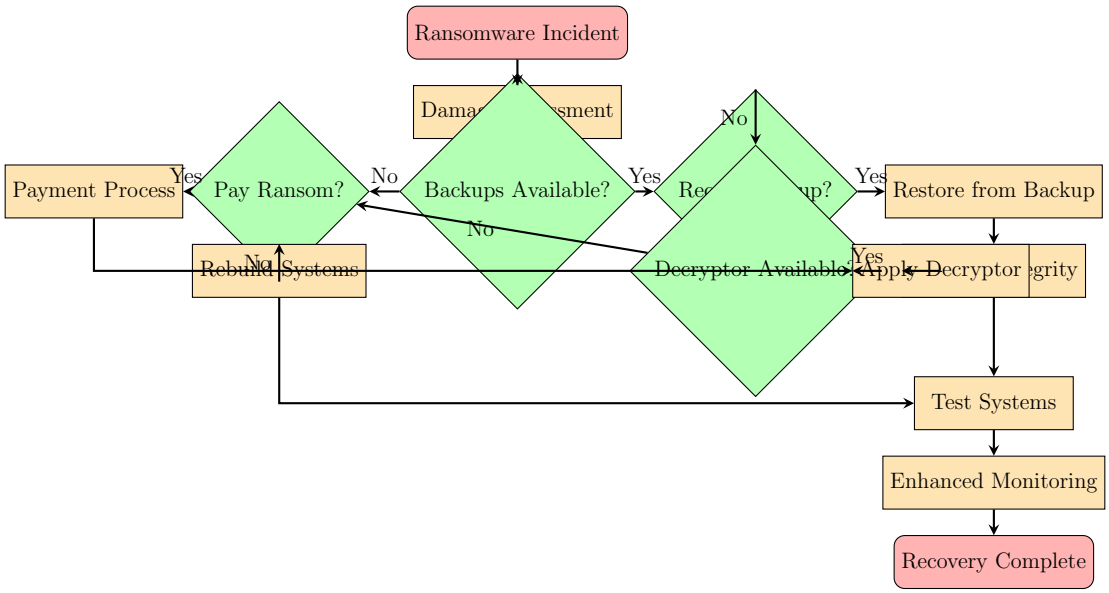


Figure 7.1: Recovery Decision Tree

7.2 System Restoration

7.2.1 Restoration Checklist

1. **Pre-Restoration:**
    - Verify malware completely removed
    - Patch all vulnerabilities
    - Reset all credentials
    - Review firewall rules
2. **During Restoration:**
    - Restore from clean backups

- Rebuild compromised systems
- Reinstall applications
- Restore data in isolated environment first

3. **Post-Restoration:**
   - Verify system functionality
   - Check data integrity
   - Monitor for reinfection
   - Update security controls

7.2.2 Backup Restoration Commands

```powershell
# PowerShell script for Veeam restoration
Add-PSSnapin VeeamPSSnapin

# Get backup repository
$repository = Get-VBRBackupRepository -Name "Primary_Repo"

# Find latest clean backup
$backup = Get-VBRBackup -Name "Critical_Servers" |
    Get-VBRRestorePoint |
    Where-Object {$_.CreationTime -lt $ransomwareTime} |
    Sort-Object CreationTime -Descending |
    Select-Object -First 1

# Start restoration
Start-VBRRestoreVM -RestorePoint $backup -PowerOn $true

# Verify restoration
$vm = Get-VM -Name $backup.VmName
if ($vm.PowerState -eq "PoweredOn") {
    Write-Host "Restoration successful" -ForegroundColor Green
} else {
    Write-Host "Restoration failed" -ForegroundColor Red
}
```

Listing 7.1: Veeam Backup Restoration

Chapter 8

Tools and Applications

8.1 Essential Security Tools

8.1.1 Detection and Analysis Tools

Table 8.1: Ransomware Detection and Analysis Tools

Tool	Purpose	Key Features
Sysinternals Suite	System monitoring	Process monitoring, autoruns analysis
Process Hacker	Process analysis	Memory strings, network connections
Wireshark	Network analysis	Packet capture, protocol analysis
IDA Pro	Malware analysis	Disassembly, debugging
YARA	Pattern matching	Malware identification rules
Cuckoo Sandbox	Dynamic analysis	Behavioral analysis in isolated environment

8.1.2 Response and Recovery Tools

Table 8.2: Incident Response Tools

Category	Tools	Usage
Forensics	FTK Imager, dd, Autopsy	Disk imaging and analysis
Memory Analysis	Volatility, Rekall	RAM forensics
Log Analysis	Splunk, ELK Stack	Centralized log management
Decryption	No More Ransom tools	Free decryptors
Backup	Veeam, Acronis	Data backup and recovery

8.2 YARA Rules for Detection

```
rule Ransomware_Generic_Indicators {
    meta:
        description = "Generic ransomware detection"
```

```
        author = "Security Team"
        date = "2024-01-01"

    strings:
        $ransom1 = "Your files have been encrypted" nocase
        $ransom2 = "Bitcoin" nocase
        $ransom3 = "Decrypt" nocase
        $ransom4 = "payment" nocase

        $crypto1 = "CryptGenKey"
        $crypto2 = "CryptEncrypt"
        $crypto3 = "CryptAcquireContext"

        $delete1 = "vssadmin delete shadows"
        $delete2 = "wbadmin delete backup"
        $delete3 = "bcdedit /set {default} recoveryenabled no"

        $ext1 = ".locked"
        $ext2 = ".encrypted"
        $ext3 = ".enc"

    condition:
        (3 of ($ransom*)) or
        (2 of ($crypto*) and 1 of ($delete*)) or
        (2 of ($ext*) and 1 of ($ransom*))
}

rule Ransomware_Conti_Specific {
    meta:
        description = "Conti ransomware detection"

    strings:
        $mutex = "kjsdf8df99s8"
        $log = "LOG:" wide
        $conti_string = "conti" nocase

    condition:
        uint16(0) == 0x5A4D and
        ($mutex or ($log and $conti_string))
}
```

Listing 8.1: YARA Rule for Ransomware Detection

Chapter 9

Communication and Escalation

9.1 Incident Communication Plan

9.1.1 Stakeholder Notification Matrix

Table 9.1: Escalation and Communication Matrix

Severity	Stakeholders	Timeframe	Method
Critical	CEO, CISO, Legal, PR	Immediate	Phone + Email
High	IT Director, Security Team	15 minutes	Email + Slack
Medium	Team Leads, Affected Departments	1 hour	Email
Low	Security Team	4 hours	Ticket System

9.1.2 Communication Templates

Initial Notification

```
Subject: [CRITICAL] Ransomware Incident Detected - Immediate
   Action Required

Incident ID: INC-2024-001
Time Detected: [TIMESTAMP]
Severity: CRITICAL
Systems Affected: [LIST]

Initial Assessment:
- Ransomware variant: [NAME/UNKNOWN]
- Scope: [NUMBER] systems affected
- Data impact: [ASSESSMENT]
- Business impact: [HIGH/MEDIUM/LOW]

Immediate Actions Taken:
- Network isolation implemented
- Incident response team activated
- Forensic evidence preservation initiated

Next Steps:
- Full investigation in progress
```

```
- Containment measures being expanded
- Recovery planning initiated

Contact: [Security Hotline]
Updates: Every 30 minutes
```

Listing 9.1: Initial Incident Notification Template

9.2 Legal and Compliance

9.2.1 Regulatory Requirements

- **GDPR:** 72-hour breach notification
- **HIPAA:** 60-day notification for healthcare data
- **PCI DSS:** Immediate notification to card brands
- **State Laws:** Vary by jurisdiction

9.2.2 Law Enforcement Engagement

1. Contact FBI IC3 or local field office
2. Preserve all evidence
3. Document timeline of events
4. Provide IoCs and malware samples
5. Coordinate public statements

Chapter 10

Testing and Validation

10.1 Tabletop Exercises

10.1.1 Ransomware Scenario

Scenario: Friday, 4:30 PM - Multiple users report unable to access files. IT discovers ransomware spreading across the network.

Table 10.1: Tabletop Exercise Checklist

Time	Action Item	Complete
T+0	Initial detection and verification	☐
T+5min	Activate incident response team	☐
T+10min	Isolate affected systems	☐
T+15min	Begin forensic preservation	☐
T+30min	Executive notification	☐
T+1hr	Scope determination	☐
T+2hr	Recovery strategy decision	☐
T+4hr	Begin restoration process	☐

10.2 Technical Validation

10.2.1 Backup Testing Procedure

```
#!/bin/bash
# Backup validation script

BACKUP_DIR="/mnt/backups"
TEST_RESTORE="/tmp/restore_test"
LOG_FILE="/var/log/backup_test.log"

# Function to test backup restoration
test_backup() {
    local backup_file=$1
    echo "$(date): Testing $backup_file" >> $LOG_FILE

    # Create test directory
```

```
    mkdir -p $TEST_RESTORE

    # Attempt restoration
    if tar -xzf $backup_file -C $TEST_RESTORE 2>/dev/null; then
        # Verify file integrity
        if find $TEST_RESTORE -type f -exec md5sum {} \; > /dev/
           null; then
            echo "$(date): Backup $backup_file validated
               successfully" >> $LOG_FILE
            rm -rf $TEST_RESTORE/*
            return 0
        fi
    fi

    echo "$(date): ERROR - Backup $backup_file validation failed!
       " >> $LOG_FILE
    return 1
}

# Test all recent backups
for backup in $(find $BACKUP_DIR -name "*.tar.gz" -mtime -7); do
    test_backup $backup
done

# Send report
mail -s "Weekly Backup Validation Report" security@company.com <
   $LOG_FILE
```

Listing 10.1: Automated Backup Testing Script

Chapter 11

Metrics and Reporting

11.1 Key Performance Indicators

Table 11.1: Ransomware Response KPIs

Metric	Description	Target	Current
MTTD	Mean Time to Detect	¡ 1 hour	____
MTTR	Mean Time to Respond	¡ 15 min	____
Containment Time	Time to stop spread	¡ 30 min	____
Recovery Time	Full restoration time	¡ 24 hours	____
Data Loss	Percentage of data lost	¡ 1%	____
Backup Success	Successful restoration rate	¿ 99%	____

11.2 Post-Incident Report Template

11.2.1 Executive Summary Dashboard

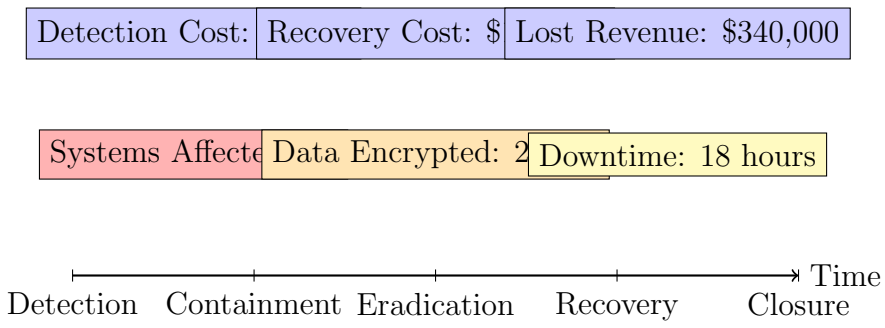


Figure 11.1: Incident Impact Summary

Chapter 12

Appendices

12.1 Appendix A: Contact Information

Table 12.1: Emergency Contact List

Role	Name	Contact	Backup
CISO	John Smith	+1-555-0100	+1-555-0101
IR Lead	Jane Doe	+1-555-0102	+1-555-0103
Legal Counsel	Bob Johnson	+1-555-0104	+1-555-0105
FBI Liaison	Agent Brown	+1-555-0106	+1-555-0107
PR Director	Alice White	+1-555-0108	+1-555-0109

12.2 Appendix B: Tool Configuration

12.2.1 Sysmon Configuration

```
<Sysmon schemaversion="4.22">
  <EventFiltering>
    <!-- Process Creation -->
    <RuleGroup name="ProcessCreate" groupRelation="or">
      <ProcessCreate onmatch="include">
        <CommandLine condition="contains">vssadmin delete</
           CommandLine>
        <CommandLine condition="contains">wbadmin delete</
           CommandLine>
        <CommandLine condition="contains">bcdedit</CommandLine>
        <CommandLine condition="contains">wmic shadowcopy</
           CommandLine>
      </ProcessCreate>
    </RuleGroup>

    <!-- File Creation -->
    <RuleGroup name="FileCreate" groupRelation="or">
      <FileCreate onmatch="include">
        <TargetFilename condition="end with">.encrypted</
           TargetFilename>
```

```
        <TargetFilename condition="end with">.locked</
           TargetFilename>
        <TargetFilename condition="contains">DECRYPT</
           TargetFilename>
        <TargetFilename condition="contains">README</
           TargetFilename>
      </FileCreate>
    </RuleGroup>

    <!-- Registry Monitoring -->
    <RuleGroup name="RegistryEvent" groupRelation="or">
      <RegistryEvent onmatch="include">
        <TargetObject condition="contains">Software\Microsoft\
           Windows\CurrentVersion\Run</TargetObject>
        <TargetObject condition="contains">Control\SafeBoot</
           TargetObject>
      </RegistryEvent>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

Listing 12.1: Sysmon Config for Ransomware Detection

12.3 Appendix C: Decryption Resources

12.3.1 Known Decryption Tools

- **No More Ransom Project:** `https://www.nomoreransom.org`
- **Emsisoft Decryptors:** Collection of free decryption tools
- **Kaspersky Decryptors:** RakhniDecryptor, RannohDecryptor
- **Trend Micro:** Ransomware File Decryptor
- **Avast:** Free ransomware decryption tools

12.4 Appendix D: Lessons Learned Template

12.4.1 Post-Incident Review Questions

1. What was the initial infection vector?
2. How long did detection take?
3. Were existing controls effective?
4. What tools failed or succeeded?
5. How was communication handled?
6. What was the business impact?

7. Were backups successful?
8. What improvements are needed?
9. Were procedures followed?
10. What training gaps exist?

Chapter 13

Conclusion

This playbook provides comprehensive guidance for responding to ransomware incidents. Regular updates, testing, and training are essential for maintaining effectiveness. Remember that prevention is always better than recovery, but when incidents occur, swift and coordinated response minimizes damage.

13.1 Document Maintenance

- **Review Frequency:** Quarterly
- **Last Updated:** December 24, 2025
- **Next Review:** [Date]
- **Owner:** Security Operations Center
- **Distribution:** Restricted - Security Personnel Only

13.2 Version Control

Table 13.1: Document Version History

Version	Date	Changes	Author
1.0	2023-01-01	Initial release	Security Team
1.5	2023-06-01	Added new tools section	John Doe
2.0	2024-01-01	Complete revision with flowcharts	Jane Smith

Bibliography

[1] NIST (2018). *Computer Security Incident Handling Guide*. Special Publication 800-61r2.

[2] SANS Institute (2023). *Ransomware: Current Threats and Responses*.

[3] CISA (2023). *Ransomware Guide*. Stop Ransomware Campaign.

[4] MITRE ATT&CK (2023). *Ransomware Techniques and Mitigations*.