AYI NEDJIMI Consultants

# Windows Forensics : Guide Expert en Analyse Securite

Catégorie : Forensics  Lecture : 4 min  Publié le : 07/12/2025  Auteur : Ayi NEDJIMI

*Étude de cas complète d Intrusion Persistante Windows Server 2025 : Analyse. Expert en cybersécurité et intelligence artificielle. Guide technique...*

## 5.1 Actions de containment immédiates

**Isolation du système compromis :** Pour approfondir, consultez Memory Forensics 2026 : Volatility 3 Avance.

```
# Script PowerShell de containment d'urgence
# Désactivation des interfaces réseau
Get-NetAdapter | Disable-NetAdapter -Confirm:$false

# Blocage des communications sortantes via Windows Firewall
New-NetFirewallRule -DisplayName "Block All Outbound" -Direction Outbound
-Action Block -Enabled True -Priority 1

# Suspension des processus suspects
$suspiciousProcesses = @("powershell", "cmd", "wscript", "cscript", "rundll32")
foreach($proc in $suspiciousProcesses) {
    Get-Process -Name $proc -ErrorAction SilentlyContinue | ForEach-Object {
        $_.Suspend()
        Write-Host "Suspended process: $($_.Name) (PID: $($_.Id))"
    }
}

# Désactivation des services malveillants identifiés
$maliciousServices = @("WinDefenderHelper", "Windows Update Helper")
foreach($svc in $maliciousServices) {
    Stop-Service -Name $svc -Force -ErrorAction SilentlyContinue
    Set-Service -Name $svc -StartupType Disabled -ErrorAction SilentlyContinue
}
```

## 5.2 Éradication des artefacts malveillants

**Processus d'éradication structuré :**

1. **Suppression des mécanismes de persistance :**

```
# Nettoyage du registre
$persistenceKeys = @(
    "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",
    "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",
    "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon",
    "HKLM:\SYSTEM\CurrentControlSet\Services"
)

foreach($key in $persistenceKeys) {
    # Audit avant suppression
    Get-ItemProperty -Path $key | Export-Csv "C:\Remediation\$
($key.Replace(':','_')).csv"

    # Suppression des entrées malveillantes
    Remove-ItemProperty -Path $key -Name "Windows Defender Update" -ErrorAction
SilentlyContinue
    Remove-ItemProperty -Path $key -Name "WinDefenderHelper" -ErrorAction
SilentlyContinue
}

# Suppression des tâches planifiées malveillantes
Get-ScheduledTask | Where-Object {$_.TaskName -match "Update|Defender|Helper"}
| ForEach-Object {
    Unregister-ScheduledTask -TaskName $_.TaskName -Confirm:$false
}

# Nettoyage WMI
Get-WmiObject -Namespace root\subscription -Class __EventFilter | Where-Object
{$_.Name -like "*Update*"} | Remove-WmiObject
Get-WmiObject -Namespace root\subscription -Class CommandLineEventConsumer |
Where-Object {$_.Name -like "*Update*"} | Remove-WmiObject
Get-WmiObject -Namespace root\subscription -Class __FilterToConsumerBinding |
Remove-WmiObject
```

2. **Suppression des fichiers malveillants :**

```
# Liste des IOCs fichiers
$maliciousFiles = @(
    "C:\Windows\Temp\update.exe",
    "C:\Windows\Temp\\14.dll",
    "C:\ProgramData\msconfig.xml",
    "C:\Users\Public\Libraries\*",
    "C:\Windows\System32\wuauhelp.dll"
)

foreach($file in $maliciousFiles) {
    if(Test-Path $file) {
        # Sauvegarde pour analyse ultérieure
        Copy-Item $file "C:\Quarantine\$(Get-Date -Format 'yyyyMMdd_HHmmss')_$
(Split-Path $file -Leaf)" -ErrorAction SilentlyContinue

        # Suppression sécurisée
        Remove-Item $file -Force -Recurse -ErrorAction SilentlyContinue

        # Vérification via ADS
        Get-Item $file -Stream * | Remove-Item -Force -ErrorAction
SilentlyContinue
    }
}
```

## 5.3 Reconstruction et durcissement

**Mesures de durcissement implémentées :**

1. **Configuration sécurisée de Windows Server 2025 :**

```
# Application des Security Baselines Microsoft
# Téléchargement et application du Security Compliance Toolkit
Install-Module -Name SecurityPolicyDsc -Force
Install-Module -Name AuditPolicyDsc -Force

# Configuration LSA Protection
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
"RunAsPPL" -Value 1

# Activation de Credential Guard
Enable-WindowsOptionalFeature -Online -FeatureName Windows-Defender-
CredentialGuard -All

# Configuration WDAC (Windows Defender Application Control)
$WDACPolicy = New-CIPolicy -Level Publisher -FilePath "C:
\Windows\System32\CodeIntegrity\WDACPolicy.xml" -UserPEs
ConvertFrom-CIPolicy -XmlFilePath "C:
\Windows\System32\CodeIntegrity\WDACPolicy.xml" -BinaryFilePath "C:
\Windows\System32\CodeIntegrity\WDACPolicy.bin"
```

2. **Implémentation de la surveillance avancée :**

```
# Configuration Sysmon pour une visibilité accrue
# Installation avec configuration SwiftOnSecurity
Invoke-WebRequest -Uri "https://github.com/SwiftOnSecurity/sysmon-config/raw/
master/sysmonconfig-export.xml" -OutFile "C:\Windows\sysmon-config.xml"
sysmon64 -accepteula -i "C:\Windows\sysmon-config.xml"

# Activation de l'audit avancé
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 /failure:enable
auditpol /set /category:"Privilege Use" /success:enable /failure:enable

# Configuration de l'audit PowerShell
Set-ItemProperty -Path "HKLM:
\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name
"EnableScriptBlockLogging" -Value 1
Set-ItemProperty -Path "HKLM:
\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" -Name
"EnableModuleLogging" -Value 1
```

3. **Segmentation réseau et Zero Trust :**

```
# Configuration des règles de pare-feu restrictives
# Blocage par défaut avec liste blanche
Set-NetFirewallProfile -All -DefaultInboundAction Block -DefaultOutboundAction
Block

# Autorisation uniquement des flux nécessaires
$allowedRules = @(
    @{DisplayName="RDP from Management Network"; Direction="Inbound";
Protocol="TCP"; LocalPort=3389; RemoteAddress="10.0.1.0/24"},
    @{DisplayName="HTTPS Outbound"; Direction="Outbound"; Protocol="TCP";
RemotePort=443; RemoteAddress="Any"},
    @{DisplayName="DNS Resolution"; Direction="Outbound"; Protocol="UDP";
RemotePort=53; RemoteAddress="10.0.0.10,10.0.0.11"}
)

foreach($rule in $allowedRules) {
    New-NetFirewallRule @rule -Action Allow -Enabled True
}
```

### 5.4 Validation post-remédiation

**Tests de validation effectués :**

1. **Scan de vulnérabilités :**

```
# Utilisation de Nessus pour validation
nessus-scan --policy "Windows Server 2025 Hardening" --target 192.168.1.100 --
report remediation_validation.pdf

# Vérification avec PowerShell
Test-NetConnection -ComputerName malicious-c2.com -Port 443 # Doit échouer
Get-Service | Where-Object {$_.DisplayName -match "Helper|Update"} # Ne doit
rien retourner
Get-ScheduledTask | Where-Object {$_.State -eq "Ready"} # Vérification des
tâches légitimes uniquement
```

2. **Monitoring continu pendant 30 jours :**

- Aucune tentative de connexion vers les IOCs réseau identifiés
- Aucune création de processus suspects
- Aucune modification non autorisée du registre
- Performances système revenues à la normale

## Phase 6 : Leçons apprises et recommandations

### 6.1 Erreurs fréquentes identifiées

**Erreurs durant l'investigation :**

1. **Contamination des preuves :**

- Exécution d'outils d'analyse directement sur le système compromis sans isolation
- Modification des timestamps lors de la copie des fichiers suspects

- Absence de documentation de la chaîne de custody

2. **Analyse incomplète :**
   - Focus uniquement sur les IOCs évidents sans recherche de variantes
   - Négligence de l'analyse des systèmes adjacents potentiellement compromis
   - Absence de recherche de backdoors secondaires
3. **Communication défaillante :**
   - Délai dans l'escalade vers le management
   - Absence de communication avec les équipes métier impactées
   - Documentation insuffisante des actions de remédiation

**Erreurs de configuration ayant facilité l'attaque :**

1. **Gestion des privilèges :**
   - Comptes de service avec des privilèges Domain Admin
   - Partages réseau avec permissions Everyone
   - Utilisation de comptes administrateur pour des tâches quotidiennes
2. **Monitoring et détection :**
   - Absence de correlation entre les événements de différents systèmes
   - Seuils d'alerte trop élevés générant des faux négatifs
   - Rétention des logs insuffisante (30 jours au lieu de 90 minimum)

### 6.2 Recommandations stratégiques

**Architecture de sécurité :** Pour approfondir, consultez LNK & Jump Lists.

1. **Implémentation d'une architecture Zero Trust :**
   - Micro-segmentation du réseau avec inspection est-ouest
   - Authentification continue basée sur le risque
   - Chiffrement de bout en bout pour toutes les communications
   - Principe du moindre privilège strictement appliqué
2. **Defence in Depth améliorée :**
   - Déploiement d'EDR sur tous les endpoints
   - SIEM avec capacités de machine learning pour la détection d'anomalies
   - Sandboxing automatique des fichiers suspects
   - Deception technology avec honeypots stratégiquement placés
3. **Résilience et récupération :**
   - Sauvegardes immutables avec air-gap
   - Plan de continuité d'activité testé trimestriellement
   - Capacité de reconstruction rapide via Infrastructure as Code
   - Environnements de test isolés pour la validation des patchs

### 6.3 Checklist de remédiation post-incident

**Checklist technique immédiate (0-24h) :**

☐ Isolation complète du système compromis

☐ Capture de la mémoire vive et création d'images forensiques

☐ Identification et isolation des systèmes potentiellement affectés

☐ Reset de tous les mots de passe des comptes privilégiés

☐ Révocation et renouvellement des certificats potentiellement compromis

☐ Blocage des IOCs réseau au niveau pare-feu et proxy

☐ Activation de l'audit avancé sur tous les systèmes critiques

☐ Déploiement de règles YARA/SIGMA pour la détection des variantes

**Actions à moyen terme (1-7 jours) :**

☐ Analyse forensique complète de tous les systèmes suspects

☐ Recherche de compromission sur l'ensemble du périmètre (Threat Hunting)

☐ Patch de toutes les vulnérabilités critiques et élevées

☐ Implémentation de la segmentation réseau d'urgence

☐ Déploiement de l'authentification multi-facteurs sur tous les comptes

☐ Configuration du monitoring renforcé avec alerting temps réel

☐ Revue et durcissement des GPO de sécurité

☐ Formation flash des équipes sur les IOCs et TTP identifiés

**Amélioration continue (7-30 jours) :**

☐ Revue complète de l'architecture de sécurité

☐ Mise à jour des procédures de réponse aux incidents

☐ Test d'intrusion ciblé sur les vecteurs identifiés

☐ Implémentation des recommandations du RCA

☐ Formation approfondie des équipes SOC et IT

☐ Mise en place d'exercices de crisis management réguliers

☐ Revue et amélioration des KPI de sécurité

☐ Établissement d'un programme de Threat Intelligence

### 6.4 Indicateurs de compromission (IOCs)

**IOCs réseau :**

```
# Domaines C2
malicious-c2.com
update-service[.]net
win-defender-updates[.]org
secure-microsoft[.]com

# IPs malveillantes
185.220.xxx.xxx (Tor exit node)
192.0.2.123
198.51.100.45
203.0.113.78

# User-Agents suspects
Mozilla/5.0 (Windows NT 10.0; Win64; x64) UpdateService/1.0
PowerShell/2.0
```

**IOCs fichiers :**

```
# Hashes SHA-256
a1b2c3d4e5f67890123456789012345678901234567890123456789012345678
b2c3d4e5f67890123456789012345678901234567890123456789012345678901a
c3d4e5f67890123456789012345678901234567890123456789012345678901ab

# Chemins suspects
C:\Windows\Temp\update.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\*.ps1
C:\Users\Public\Libraries\*.dll
C:\Windows\System32\wuauhelp.dll
```

**Règles YARA :**

```
rule APT_Malware_Persistence {
    meta:
        description = "Detects persistence mechanisms used in the attack"
        author = "Security Team"
        date = "2025-09-20"

    strings:
        $a1 = "powershell -nop -w hidden -enc" nocase
        $a2 = "WinDefenderHelper" wide
        $a3 = "Windows Update Helper" wide
        $b1 = {73 76 63 68 6F 73 74 2E 65 78 65 20 2D 6B} // svchost.exe -k
        $c1 = "FromBase64String" nocase
        $c2 = "IEX" nocase
        $c3 = "DownloadString" nocase

    condition:
        2 of ($a*) or (1 of ($a*) and 1 of ($b*)) or all of ($c*)
}
```

**Ressources open source associées :**

- SuperTimelineBuilder — Générateur de super timeline (C++)
- LogParser-AI — Analyse de logs avec IA (Python)
- IncidentSummarizer — Résumé d'incidents avec IA (Python)
- forensics-windows-fr — Dataset forensics Windows (HuggingFace)
- incident-response-fr — Dataset réponse à incident (HuggingFace)

## Questions frequentes

### Comment mener une investigation forensique sur un systeme compromis ?

Une investigation forensique debute par la preservation des preuves via une image disque et un dump memoire, suivie de l'analyse des artefacts systeme (registres, journaux d'evenements, fichiers prefetch), la reconstruction de la timeline d'activite et la correlation des indicateurs de compromission pour identifier la source et l'etendue de l'attaque.

### Quels sont les outils essentiels pour l'analyse forensique ?

Les outils essentiels pour l'analyse forensique incluent Volatility pour l'analyse memoire, Autopsy et FTK pour l'analyse disque, KAPE et Velociraptor pour la collecte automatisee, Plaso pour la creation de timelines, ainsi que des outils de triage comme Eric Zimmerman's tools pour l'analyse des artefacts Windows.

### Pourquoi la chaine de custody est-elle importante en forensique ?

La chaine de custody garantit l'integrite et l'admissibilite des preuves numeriques en documentant chaque etape de manipulation, de la collecte a la presentation. Sans une chaine de custody rigoureuse, les preuves peuvent etre contestees juridiquement et perdre leur valeur probante.

Pour approfondir, consultez les ressources de CERT-FR et de NIST Cybersecurity.

**Sources et références :** SANS SIFT · MITRE ATT&CK

Articles connexes

- Email Forensics : Tracer les Campagnes Phishing en 2026
- Registry Forensics : Guide Expert Analyse Securite

## Conclusion

Cette étude de cas illustre la complexité d'une intrusion moderne utilisant des techniques poussées d'évasion et de persistance. L'incident a mis en évidence plusieurs défaillances critiques dans l'architecture de sécurité, notamment l'exposition de services sensibles, l'absence de segmentation réseau appropriée et des pratiques de gestion des privilèges inadéquates.

L'investigation forensique approfondie a permis non seulement d'éradiquer complètement la menace mais aussi d'identifier les faiblesses systémiques ayant permis l'intrusion. Les recommandations issues de cette analyse ont conduit à une refonte significative de la posture de sécurité de l'organisation, incluant l'adoption d'une architecture Zero Trust, le renforcement du monitoring et la mise en place de processus de réponse aux incidents plus robustes.

Les leçons tirées de cet incident soulignent l'importance cruciale d'une approche proactive de la cybersécurité, combinant des mesures préventives robustes, une capacité de détection avancée et une préparation adéquate à la réponse aux incidents. La documentation détaillée de cet incident servira de référence pour améliorer continuellement les capacités de défense et de réponse de l'organisation.

L'évolution constante des menaces nécessite une vigilance permanente et une adaptation continue des stratégies de sécurité. Cet incident rappelle que même avec Windows Server 2025 et ses améliorations de sécurité, la configuration appropriée, la surveillance active et la réponse rapide restent essentielles pour maintenir une posture de sécurité efficace.

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr