SCRIPT #12 · CYBER SECURITY

File modificati di recente (indicatore ransomware)

Cerca file modificati in un intervallo sospetto e in numero elevato, indicatore possibile di ransomware attivo.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Permessi di lettura sui percorsi analizzati

Cosa fa questo script

Lo script scandisce ricorsivamente uno o piu percorsi specificati alla ricerca di file modificati negli ultimi N minuti, raggruppando i risultati per cartella. Un numero elevato di modifiche concentrate in un breve lasso di tempo, su molte cartelle diverse, e un pattern tipico dell'attivita di cifratura di un ransomware.

Come si usa

Specifica uno o piu percorsi da analizzare e la finestra temporale (in minuti) da considerare sospetta.

```
.\Scan-FileModificatiRecenti.ps1 -Percorsi "D:\Condivisioni" -MinutiIndietro 15
```

In quale contesto usarlo

Da usare come controllo diagnostico immediato quando si sospetta un'infezione in corso (utenti che segnalano file illeggibili, estensioni cambiate), oppure schedulato come controllo ricorrente su condivisioni critiche per un rilevamento precoce, sapendo pero che non sostituisce un vero EDR dedicato.

Codice completo

Il codice è lo stesso del file Scan-FileModificatiRecenti.ps1: per usarlo scarica il file dalla pagina invece di copiarlo da questo PDF.

```
<#
.SYNOPSIS
    Cerca file modificati in un intervallo di tempo sospetto, indicatore possibile di ransomware attivo.
#>
param(
    [Parameter(Mandatory=$true)]
    [string[]]$Percorsi,
    [int]$MinutiIndietro = 15,
    [int]$SogliaFileSospetta = 50,
    [string]$PercorsoCSV = "C:\Report\FileModificatiRecenti.csv"
)

$dataLimite = (Get-Date).AddMinutes(-$MinutiIndietro)

$fileModificati = foreach ($percorso in $Percorsi) {
    Get-ChildItem -Path $percorso -Recurse -File -ErrorAction SilentlyContinue |
        Where-Object { $_.LastWriteTime -gt $dataLimite }
}

$perCartella = $fileModificati | Group-Object DirectoryName | Sort-Object Count -Descending

$riepilogo = $perCartella | Select-Object @{N="Cartella";E={$_.Name}}, Count
```

```
$riepilogo | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"

$cartelleSospette = $perCartella | Where-Object { $_.Count -ge $SogliaFileSospetta }
if ($cartelleSospette) {
    Write-Host `
        "[ALLARME] $($cartelleSospette.Count) cartelle con oltre $SogliaFileSospetta modifiche negli ultimi $MinutiIndietro minuti!" -ForegroundCol
} else {
    Write-Host "Nessuna cartella supera la soglia di $SogliaFileSospetta modifiche in $MinutiIndietro minuti." `
        -ForegroundColor Green
}
```