コマンドの内容を分解

`reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Shell /d "explorer.exe, C:\windows\tasks\dwm.exe" /f`

各要素の意味

部分	意味
`HKLM\...\Winlogon`	**ログオン処理を司る超重要レジストリ**
`Shell`	ユーザーがログイン後に起動されるシェル
`explorer.exe`	正常な Windows シェル
`, C:\windows\tasks\dwm.exe`	**追加で起動させる不正実行ファイル**
`/f`	強制上書き

なぜ危険か（重要）

正常な値

`Shell = explorer.exe`

今回の値

`Shell = explorer.exe, C:\windows\tasks\dwm.exe`

👉 **ログインするたびに `dwm.exe` が自動実行**されます。

悪質なポイント

① 正規プロセス名の偽装

- `dwm.exe` は本来 `C:\Windows\System32\dwm.exe`
- 今回は `C:\windows\tasks\dwm.exe`

➡ 完全ななりすまし

---

② 実行場所が異常

- `C:\Windows\Tasks\` は
  - 旧来のタスク関連フォルダ
  - **攻撃者が好む隠し場所**

---

③ 高権限・高信頼な永続化

- `HKLM` 配下 → **管理者権限必須**
- Winlogon → **EDR回避されやすい**
- ログオン時に確実実行

サイバーキルチェイン上の位置

フェーズ	該当
Persistence	✅
Privilege Escalation	間接的
Defense Evasion	✅

MITRE ATT&CK

- `T1547.004` – Winlogon Helper DLL / Shell

Splunkでの検知SPL（単語ベース）

```
index=* CommandLine="*Winlogon*Shell*explorer.exe,*"
```

もう少し厳密

```
index=* CommandLine="*reg*add*Winlogon*Shell*" NOT CommandLine="*explorer.exe\"
```

index=
CommandLine="Winlogon*Shell*explorer.exe,*"
① このSPLが何をしているか（超要約）
👉 Winlogon の Shell レジストリに対して、
explorer.exe の後ろに「何か」を追加しているコマンドを探しています。

＝ ログオン時に不正プログラムを自動実行させる永続化の痕跡

② CommandLine 条件を分解
CommandLine="*Winlogon*"
対象：

コードをコピーする
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
ログオン処理を司る超重要レジストリ

通常の業務ではほぼ触られない

Shell
Shell 値は ログイン後に起動されるプログラム

正常値：

コードをコピーする
explorer.exe
explorer.exe,
ここが 最重要ポイントです。

なぜカンマ（,）が重要？
Windows は Shell 値を カンマ区切りで複数実行できます。

text
コードをコピーする
Shell = explorer.exe, evil.exe
➡ explorer.exe の起動に紛れて悪意のある exe を実行

③ なぜこのSPLは強いのか
正常ではヒットしない
状態 ヒット
Shell = explorer.exe ❌
Shell = explorer.exe, evil.exe ✅
Shell = evil.exe ❌（このSPLでは）

👉 誤検知が極めて少ない

④ 攻撃者がこの手法を使う理由
理由 説明
高い永続性 ログオン毎に確実実行
高信頼 explorer.exe に偽装
EDR回避 古典だが検知が甘い環境あり
管理者前提 侵害が深い証拠

⑤ サイバーキルチェイン上の位置
Persistence（永続化）

Defense Evasion（防御回避）

MITRE ATT&CK

T1547.004 – Winlogon Shell

⑥ どんなログでヒットする？
主なソース
Security Event Log（4688）

Sysmon（EventCode=1）

EDR（Process Creation）

例（ヒットログ）
text
コードをコピーする
CommandLine:
reg add "HKLM...\Winlogon" /v Shell /d "explorer.exe, C:\Windows\Tasks\dwm.exe" /f
⑦ 改良版SPL（より安全）
explorer.exe 以外が混ざっている場合を検知
spl
コードをコピーする
index=
*CommandLine="*Winlogon*Shell*explorer.exe,*"*
*NOT CommandLine="*System32\explorer.exe""
explorer.exe 単体以外をすべて拾う
spl
コードをコピーする
index=
*CommandLine="*Winlogon*Shell*"
NOT CommandLine="*Shell" /d "explorer.exe"*"
⑧ 検知後に必ずやること
Shell の現在値確認

c
コードをコピーする
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Shell
explorer.exe 以外の実体確認

署名・ハッシュ確認

作成者・親プロセス追跡

横展開確認