脅威ハントの過程で、環境内で3つの侵害されたシステムを特定しました。
WK3
DB01

タイムライン

| タイムスタンプ | 観察 | 影響を受ける資産 |
|---|---|---|
| 2025/05/30 12:20:30 AM | SYSTEM 権限の App.exe が J_James_Tax_Return_Final_Review.docm を C:\Windows\System32\wwwroot\uploads\ に作成 | APPSRV01 |
| 2025/05/30 12:20:38 | マルウェア実行　Word（WINWORD.EXE）から radF02DD.tmp.exe が Temp 配下で実行 | WK02 |
| 2025/05/30 12:20:38 | 親プロセスが Word、子プロセスがランダム名 exe。業務文書を装った初期侵入 | WK02 |
| | | WK02 |
| | | 内部ネットワーク |
| | | DC01 |
| | | DC01 |
| [...] | [...] | [...] |

IOCs

添付は、脅威ハンティングスプリント中に検出された結果のIOCのまとめリストです。

### ファイルハッシュ

| ファイル名 | SHA256 |
|---|---|
| J_James_Tax_Return_Final_Review.docm | |
| radF02DD.tmp.exe | |
| dwm.exe | |
| certutil.exe | |

### ネットワーク通信

| 種類 | 価値 |
| --- | --- |
| C&C | 192.168.12.231 |
| ファイルダウンロード | J_James_Tax_Return_Final_Review.docm |
| ファイルダウンロード | radF02DD.tmp.exe |
| ファイルダウンロード | dwm.exe |
| ファイルダウンロード | certutil.exe |