- 先にやるべきことはフラグ！！
- だから、コピペくらいでとめておく。
- フラグ関係はクエリとキャプチャをとる
- それ以外は、最後にエビ一気に再現

問題

1. 攻撃者が Quickfile.inc 環境への最初のアクセスを取得するために使用した悪意のあるファイルの名前は何ですか?
2. 攻撃者が攻撃ツールを Quickfile.inc 環境に転送するために使用するスクリプト、アプリケーション、またはコマンドレットの SHA-256 ハッシュは何ですか?
3. 攻撃者は、権限昇格や横展開といった特定のアクションの後に、様々な永続化メカニズムを利用することで知られています。Quickfile Inc 環境で利用されている永続化メカニズムとして使用されるオブジェクトの名前は何ですか？オブジェクトとは、ファイル名、レジストリキー、ユーザー名、スケジュールされたタスク名などです。（形式：パス、ドメイン名、コンピュータ名、デバイス文字などのプレフィックスやサフィックスを含まない ObjectName）
4. 攻撃者が Quickfile.inc 環境への永続性を確立するために使用した実行可能ペイロードの SHA-256 ハッシュは何ですか?
5. 攻撃者がQuickfile.inc環境に最初にアクセスしたファイルまたは実行可能ペイロードは、いつ最初に実行されましたか？タイムスタンプを入力してください。
6. 攻撃者が Active Directory 環境の完全な侵害を可能にする情報を収集するために使用したスクリプト、アプリケーション、またはコマンドレットの SHA-256 ハッシュは何ですか?
7. 攻撃者は1台以上の外部マシンを悪意のある目的で使用しました。攻撃者が使用したホスト名、DNS名、またはIPアドレスは何ですか？

   192.168.12.231
   J_James_Tax_Return_Final_Review.docm
   radF02DD.tmp.exe
   dwm.exe
   certutil.exe

タイムライン

時間	端末	イベント	概要	内容詳細
2025/05/30 12:20:30 AM	APPSRV01	ファイル作成	マクロ付き文書生成	SYSTEM 権限の App.exe が J_James_Tax_Return_Final_Review.docm を C:\Windows\System32\wwwroot\uploads\ に作成
2025/05/30 12:20:38	WK02	プロセス作成	マルウェア実行	マルウェア実行　Word（WINWORD.EXE）から radF02DD.tmp.exe が Temp 配下で実行
2025/05/30 12:20:38	WK02	初期侵入	マクロ悪用	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
2025/05/31 9時台	WK02	資格情報取得	AS-REP Roasting	Rubeus を用いた Kerberos AS-REP Roasting 実行を確認
2025/05/31 9時台	内部ネットワーク	内部偵察	AD 情報収集	SharpHound / PowerView 等を使用し AD 構成・権限関係を調査
2025/05/31 13:55:19	DC01	アカウント作成	永続化	新規ユーザー m.williams が作成される、永続化 r.williams
2025/05/31 13:55:19	DC01	バックドア	永続化	通常ユーザーを装ったバックドア用アカウント

時間	端末	イベント	概要	内容詳細

時間	端末	イベント	概要	内容詳細

気づき

実行ログ