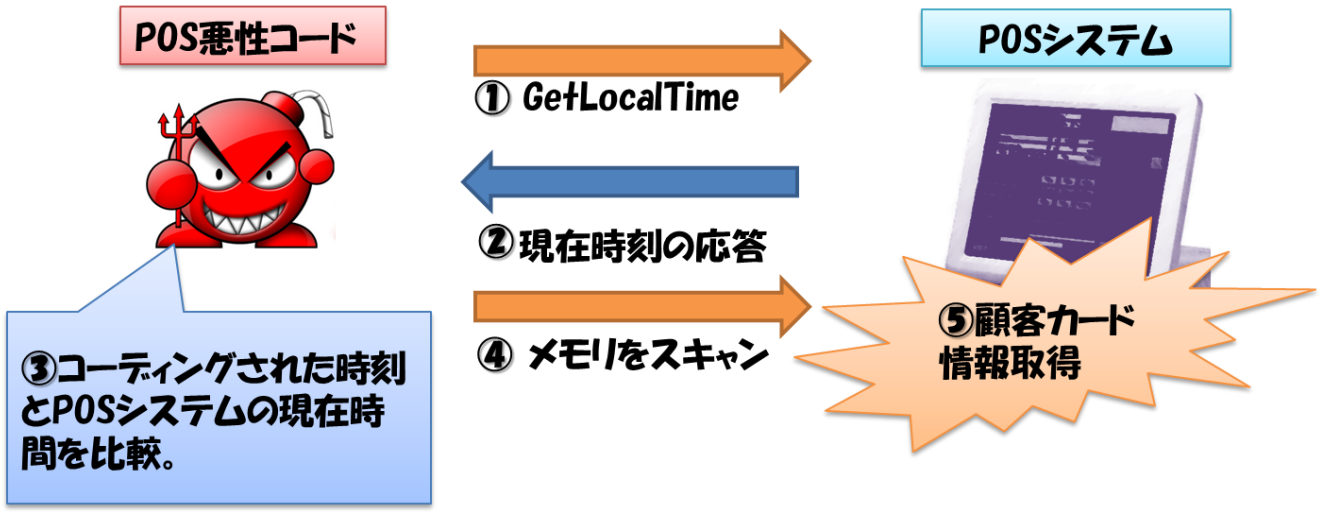
2015 年 5 月 1 日
株式会社セキュアソフト

悪性コード：特定の時間に動作する POS システム向け悪性コード

1. 概要

POS(Point of Sale)システムを対象としている悪性コードが増加傾向となっておりますが、Windows ベースの POS システムに対して特定の時間に動作する悪性コードが発見されました。POS システムが該当の悪性コードに感染した場合、システムの時間と悪性コードにコーディングされた特定の時間を比較して悪性コードの時間が早い場合は POS システムのメモリをスキャンして POS システムにあるカード番号を取得します。

2. 攻撃の流れ



① 攻撃対象の POS システムに GetLocalTime を利用して対象の時間を取得します。
② POS 悪性コードの内部にコーディングされた Timestamp と①で確認した POS システムの時間を比較します。
③ 比較の結果、POS システム時間が早い場合、POS 悪性コードは exe ファイルを利用してメモリ情報をスキャンします。
④ メモリをスキャンした後に生成されたタップファイルに関して正規表現を利用してカード情報を取得します。

3. まとめ

2015 年に新しく出現した POS 悪性コードは特定の時間に動作するように精巧に準備されています。POS システムを攻撃対象としたツール（ex.ファイルやメモリをスキャンするツール）はインターネットから容易に入手することが可能です。攻撃者はインターネットから入手した様々なツールから亜種の悪性コードを作成して第 2、第 3 の攻撃を行う事も可能です。POS システムを利用するユーザは被害を削減するためのセキュリティ対策が必要です。