【Technical Report】
シグネチャリリース

2015 年 6 月 24 日
株式会社セキュアソフト

2015 年第１０回シグネチャリリース

本日、標的型攻撃で使用されるマルウェアを検知するシグネチャを含む 11 件のリリースをしました。

<シグネチャ名>

- **Win32/Backdoor.EMDIVI.Connection.C**
- **Win32/Backdoor.EMDIVI.Connection.B**
- **Win32/Backdoor.EMDIVI.Connection.A**

<攻撃の説明>

標的型攻撃で用いられる不正コード(マルウェア)により、%TMP%環境変数で指定されたフォルダ以下に無害な文書ファイルを生成して実行させ、その後不正行為を行う不正コードを生成する。再起動後も継続して不正行為を行うためスタートアップフォルダに不正コードを実行させるための lnk ファイルを生成する。

当該不正コードの動作により、C&C サーバと HTTP POST, GET, HEAD メソッドを利用して通信し、ユーザ情報などが奪取される恐れがある。

SecureSoft Sniper IPS をご利用のお客様は、自動アップデート、手動アップデートにより最新シグネチャを適用してご利用下さい。

以上