【Technical Report　15-005】
悪性コード情報

2015 年 5 月 22 日
株式会社セキュアソフト

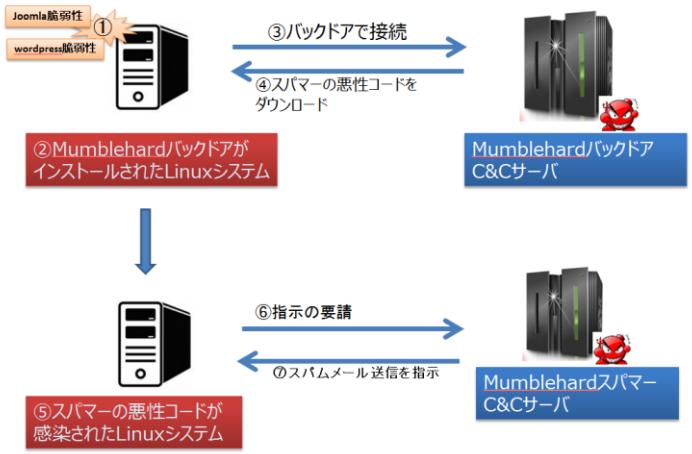
悪性コード：Linux/Mumblehard について

1. 攻撃説明

Mumblehard はバックドアとスパマー機能を持っている悪性コードです。 Linux システムが Mumblehard に感染すると、バックドアにより C&C サーバに接続して、スパマーの悪性コードをダウンロードします。その結果 Proxy サーバを通じてスパムメールを配布するボットとなります。

Mumblehard は Perl Script ベースの不正コードにパッケージングされており、Yellsoft 社の DirectMailer 機能を利用してスパムメールを発送します。Mumblehard は感染経路で joomla 脆弱性、wordpress 脆弱性を利用するほか、不正に複製した Direct Mailer をインストールする際に感染する可能性があります。

システムが Mumblehard に感染すると、異常なデーモンが cron ジョブに登録されます。cron ジョブに登録された異常なデーモンは、15 分間隔で C&C サーバと通信するためのバックドアを有効化します。通常、Mumblehard バックドアは /tmp, /var/tmp のディレクトリにインストールされます。



2. 対策方法

C&C ドメインと Yellsoft 社の DirectMailer による感染を防ぐため、Yellsoft email に係る不正ドメインの IP アドレス通信を遮断します。この対策により C&C サーバとの通信停止し、Linux システムにスパマーの悪性コードのダウンロードをしないように対応します。

3. SniperIPS による対策

Mumblehard の感染経路である joomla 脆弱性、wordpress 脆弱性を検知する Sniper IPS のシグネチャを利用して Mumblehard のバックドアがインストールされる前に遮断する対策が可能です。

以上