2015 年 4 月 3 日
株式会社セキュアソフト

新たな脅威 RansomWeb について

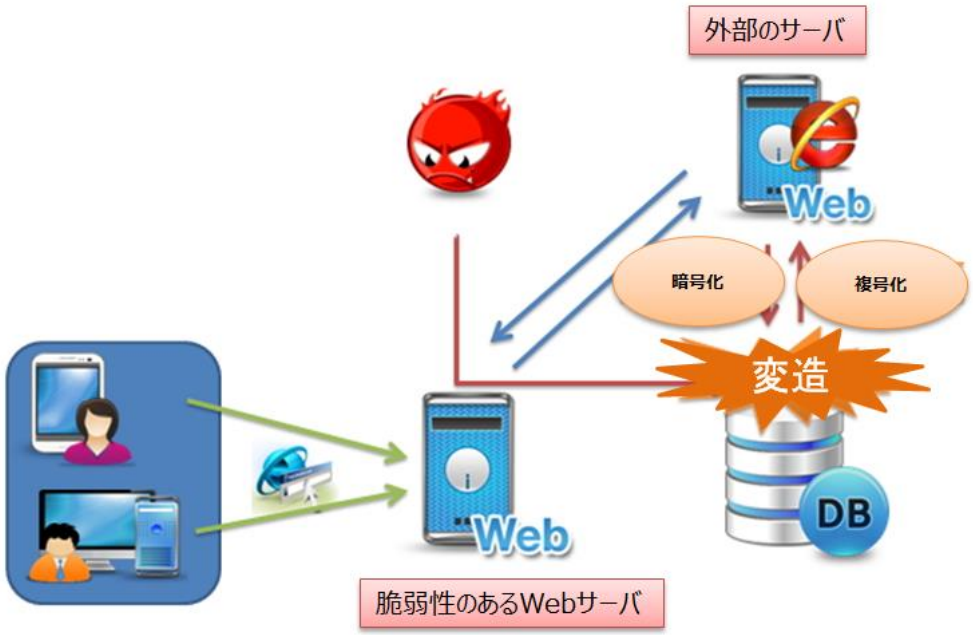
1. 概要

PC を狙った Ransomware による攻撃が増加していますが、Web サーバの DB をターゲットとする RansomWeb 攻撃が確認されました。

2. RansomWeb の内容

Ransomware の場合は、PC の重要なファイルを攻撃者が暗号化し、データを人質として、解除パスワードと交換でお金を要求する攻撃ですが、RansomWeb の場合は Web サーバを対象としてサーバの DB を暗号化することでより広範囲に影響を及ぼす攻撃です。

攻撃者は脆弱性のある Web サーバを利用して DB に関する情報を把握した後、外部のサーバを利用して DB の暗号化を実施します。



3. 攻撃の影響

攻撃を受けた web サーバは意図せず DB が暗号化されるため、DB から正常な情報を取得することが出来ず、サービス提供が不能状態になります。

さらに暗号化された情報は複号化する事が出来ず、復旧のため攻撃を受ける前の時点に DB をロールバックすることになるため、情報の損失や復旧にかかるコスト等が発生します。

4. 影響度

現在確認されている攻撃対象は PHP 環境のサーバですが、他の環境でも攻撃を受ける可能性があります。

① ASP, JSP の環境に対して Custom された ASP,JSP 関数を利用した RansomWeb 攻撃を行う場合

② PHP Web サーバと連動している DB を共有する環境の場合

5. 対応策

RansomWeb 攻撃は Web サーバの脆弱性を利用して、Web サーバの管理権限を取得されることが原因です。

基本的な対策は Web サーバの脆弱性に関する定期的なパッチ管理となりますが、攻撃者はスキャニング行為により事前に Web サーバの脆弱性に関する情報を取得するため、IPS などによるプロアクティブな対応も重要です。攻撃を受けた可能性のある場合はただちに重要なファイルから整合性検査を実施してファイルの偽造と変造を確認する必要があります。