Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 28 年1月 13 日

Topic

NoSQLデータベースであるRedisを標的としたアクセスについて

インターネットに接続されている Redis を標的としたアクセスを観測しました。Redis に対する危険性が公表されており、対策が不十分な場合、Redis が不正に操作され、Redis が稼動するサーバ上にファイルが蔵置される可能性があります。Redis を利用している組織や個人は、適切な対策を実施することを推奨します。

1 公表された Redis の危険性について

Redis[i]は、オープンソースで開発及び公開されている NoSQL[ii]データベースです。

平成 27 年 11 月4日に、Redis の開発者のウェブサイトにおいて、インターネットに接続されている Redis が不正に操作され、外部からファイルを蔵置される危険性が公表[iii]されました。同ウェブサイトには、当該危険性を実証するための具体的な手順や使用するコマンド等の手法が示されていました。また、当該手法により、外部から SSH の公開鍵が蔵置された場合、SSH による接続を許してしまうとのことです。

2 Redis を標的としたアクセスの観測について

定点観測システムでは、平成 27 年 11 月 14 日から、同ウェブサイトで示された危険性に係る手法の特徴を有するアクセスを観測しました(図、表)。これらのアクセスを分析したところ、Redis が稼動しているサーバ上にファイルの蔵置を試みていると考えられる複数のコマンドが含まれていました。

---

i Redis
http://redis.io/

ii 一般的には「Not only SQL」の略とされ、ビックデータ等の膨大なデータを高速に扱えるように考案された、既存のデータベースとは異なる、性能や特性を持つ新たなデータベースの総称。

iii 「A few things about Redis security」
http://antirez.com/news/96

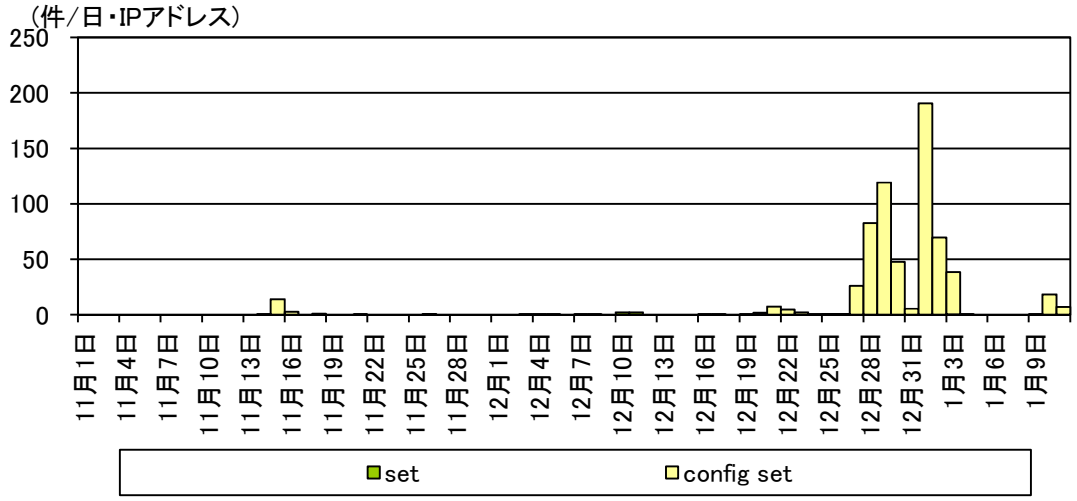

図　Redis の探索が目的と考えられるアクセス件数の推移（コマンド別）
（H27.11.1～H28.1.11）

表　観測された Redis のコマンドの機能

コマンド名	コマンドの機能
set	文字列値（データ）をキーにセットする。
config set	サーバの設定変更を行う。変更された設定は、直ちに反映される。

3　推奨する対策

Redis を利用する組織や個人においては、Redis を外部に公開している場合、外部から接続されコマンドを実行される危険性があるため、以下のような対策を実施することを推奨します。

- Redis を外部に公開する必要がある場合は、必要なコンピュータからのみアクセスを可能とするなど適切なアクセス制限を実施する。
- 容易にコマンドが実行されることを防ぐために、適切なパスワードをあらかじめ設定しておく。
- ファイルの蔵置は、Redis を起動しているユーザ権限で実行されるため、当該ユーザの権限を必要最小限とした上で起動するなどの設定を行う。