Java Deployment Toolkit の未修正の脆弱性と「いわゆるGumblar」について

2010年11月25日

一般社団法人 JPCERTコーディネーションセンター
水野哲也

概要

- 2010年4月にJava Deployment Toolkit の未修正の脆弱性を攻撃する手法が、「いわゆるGumblar」に組み込まれる事例が発生

- IBM 東京 SOC様から提供いただいた情報をもとに、攻撃に使用されたサイトを特定し、サイトの管理者にサイト停止の為のコーディネーションを実施
  - マルウエアが設置されているサイト
  - ID パスワードの送信先サイト

最初は…

JPCERT CC®

- 2010年4月9日
  - Java Deployment Toolkit の引数検証処理に関する脆弱性情報が公開（修正プログラムは無し）
    - Java SE 6 update 19（4月9日時点で最新）以前に影響

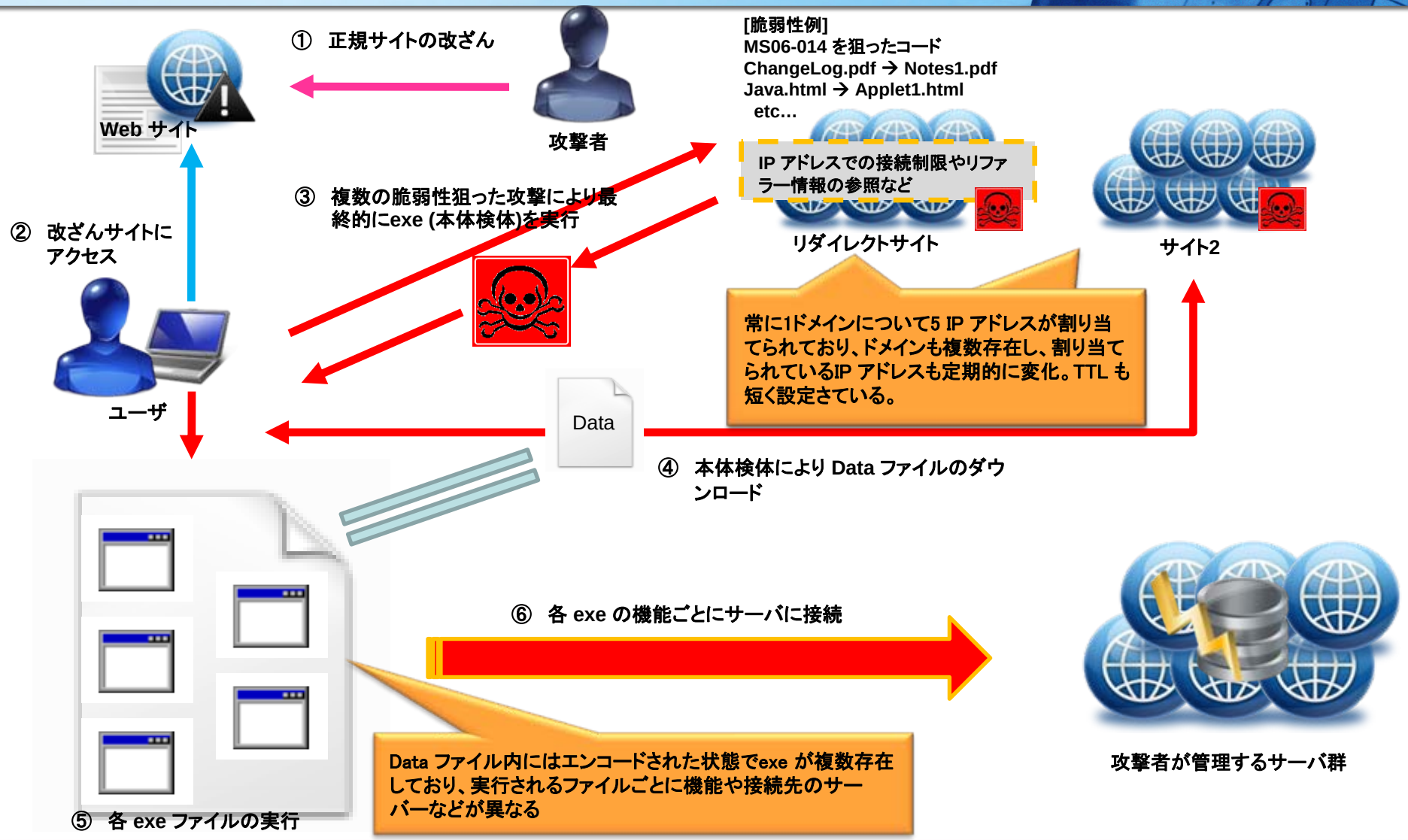
- 2010年4月12日
  - 公開された実証コード(以下、PoC)の情報を入手
    - Java SE 6 update 19以前の環境で任意のコードが実行できることを確認
    - PoCは、samba などのファイル共有のディレクトリに置かれている *jar ファイルを実行する仕組みになっていた
  - 12日時点で、この脆弱性が攻撃に使用されたことを観測していなかった

脆弱性がいわゆるGumblarに組み込まれる

JPCERT CC®

- 2010年4月15日
  - IBM 東京 SOC様にて「Java Deployment Toolkitの脆弱性を悪用したゼロディ攻撃を観測」のレポートを公開
    - 「いずれも8080ポートを利用したドライブ・バイ・ダウンロード攻撃の過程で、他の脆弱性への攻撃とともに実施されており、国内の企業環境で被害が観測されています。」
    - https://www-950.ibm.com/blogs/tokyo-soc/entry/javaws-201004?lang=ja
  - Oracle社から Java SE 6 update 20が公開
    - 先に修正プログラムが公開（公式のセキュリティアドバイザリは未公開）
    - Java SE 6 update 20を適用するとPoCが動作しないことを確認
  - JPCERT/CCから重要インフラ事業者に、早期警戒情報を提供

Gumblar.8080の攻撃の流れ



IBM 東京 SOC 様から情報提供

JPCERT CC®

- 2010年4月15日
  - IBM 東京 SOC様から事例に関する情報を受領
    - Redirector、Injector などの情報
  - 提供いただいた情報をもとに攻撃の挙動と、攻撃に使用されたサイトを特定し、当該サイトの管理者に対して、サイトの停止の為の調整（コーディネーション）を開始
    - *.jar ファイルを公開していたサイト
      - 4箇所（NL 2、US 1、LV1）
    - 感染後に ID、パスワード情報を送信する先のサイト
      - 1箇所（IT）

その後

JPCERT CC®

- 2010年4月16日
  - Oracle社からセキュリティアドバイザリが公開
    Oracle Security Alert CVE-2010-0886
    http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0886.html
  - JPCERT/CCから注意喚起を発行
    - Oracle Sun JDKおよびJREの脆弱性に関する注意喚起
    - http://www.jpcert.or.jp/at/2010/at100010.txt
  - IBM 東京 SOC様から追加の情報をいただく
    - 新たに攻撃に使用されたサイトに対してコーディネーションを開始

- 2010年4月17日 以降
  - 「いわゆるGumblar」の挙動に変化がないかを継続して情報収集
  - 新たな攻撃を発見し次第、新たな jar ファイルの設置サイトや通信先のサイトへのコーディネーションを実施

最後に

- 今後も、未修正の脆弱性が「いわゆるGumblar」などの攻撃に組み込まれるケースが発生する可能性があります。

- 被害拡大を防ぐには、迅速な情報共有と対応が必要です。改ざんされたサイトなどを発見した場合は情報提供をお願いします。

  - JPCERT/CC へのインシデントの報告やご相談
    報告について：https://www.jpcert.or.jp/form/
    Webフォーム：https://form.jpcert.or.jp/
    Email　　：info@jpcert.or.jp