【Technical Report 15-001】
悪性コード情報

2015 年 3 月 20 日
株式会社セキュアソフト

悪性コード情報：Linux/DDoS.XorDDoS

1. 概要

Linux/DDoS.XorDDoS は侵入先のコンピュータで悪質な操作を実行する可能性がある悪性コードです。
Linux Kernel 3.x.x, 2.x.x をはじめ、他の Linux Kernel バージョンでも不正行為の影響を受ける可能性があります。

2. 攻撃手法

Linux/DDoS.XorDDos は、XorDDoS 攻撃に使用される悪性コードです。

発見された攻撃手法では、攻撃者が脆弱なアカウントの Linux 系サーバからシステム権限を奪取し、そのサーバに今回の攻撃に使う Shell Script 実行及び悪性コードのダウンロードを行います。悪性コードをダウンロードする際、システムが既に感染されているかを確認し、感染されていなければ、当該システム環境に合わせた悪性コードを追加で作成するため攻撃者のサーバに Kernel バージョン情報を転送します。その後、ダウンロードした悪性コードは XorDDoS Bot として C&C サーバと通信し、TCP, UDP 通信パケットを使用した DDoS 攻撃を行います。この悪性コードは正常なライブラリファイルに偽装するため、自身をコピーします。さらに、システム終了時に自動実行ができるように不正な環境を作る等さまざまな仕掛けをとっていることが発見されています。

3. 対策案

１）いくつかの特定ディレクトリにランダムな英文字 10byte 名前のファイルがあります。
　そのファイルを手動で削除します。
２）いくつかの特定スタートスクリプトディレクトリにランダムな英文字 10byte の名前のスタートスクリプトファイルがあります。
　そのスクリプトを手動で削除します。

4. Sniper IPS の対応

Sniper IPS ではこの攻撃を検知・防御する以下のシグネチャーを提供しています。

対応シグネチャー名
Linux/DDoS.XorDDos.CompileCheck
Linux/DDoS.XorDDos.InfectedCheck

本内容の詳細についてお問合せいただく場合、Sniper シリーズをご利用のお客様は販売代理店様、ご契約のサポート窓口を通じて弊社技術サポートへご連絡をいただけますようお願いいたします。

以上