

rootkit 調査報告書

2002.12

概要

rootkit とはコマンド改ざんツール、サーバプログラム（バックドア、DDoS、ファイル交換など）、スニファなどと インストーラのセットである。

rootkit 利用には root 権限でシェルを実行できることが前提となる。

一般的な rootkit

UNIX 系の場合不正常駐プロセス、不正コマンドの検知を防ぐ手法により 2 タイプある。以下にあげたもの以外の亜種が多数存在する。

- ・ ps,ls,netstat などシステムコマンドファイルを改ざんをするタイプ
t0nkit など
- ・ LKM (Loadable Kernel Module) でシステム関数をのっとるタイプ
knark、lrk など

Windows も同様にタスクマネージャなどの exe を置き換え、不正プロセスを隠蔽し、システム関数をのっとるタイプがある。

- ・ NT rootkit など

検出

検出作業のきっかけには、他サイトからの不正アクセス報告、ネットワーク機器、IDS 等によるイベント通知、ログ解析結果などが挙げられる。

被攻撃サーバが不正プログラムに汚染されていないことを証明するのは困難である。特に、新たなタイプの不正プログラム検出が既存のツールで検出可能かは未知である。

UNIX 系においてのシステム関数改ざんの場合、被攻撃サーバでのサービス停止を伴わない検出は困難である。正常なカーネルで被攻撃サーバのハードディスクをマウントし調査する必要がある。しかし、システム停止を行って、調査・リストアを実施する決断を下すには、事前に相応の被攻撃証拠が必要である。

サーバに被攻撃証拠がない場合も、インシデント後一定期間ネットワーク機器のログチェックやネットワークモニタによる解析が必要である。

検知ツール：システム停止なしで利用可能なもの

- ・ スタティックリンクにより作成した正常コマンド
 - ps,ls,netstat などのシステムコマンド
- ・ ファイル改ざん検出ツール
 - Tripwire：ハッシュ値保存・管理ツール：他機器との連携が可能
- ・ rootkit 検出ツール
 - chkrootkit：各種 OS ステータスコマンド、シグネチャベース検出
 - kstat：対 LKM - システム関数アドレスチェック
 - alamo：対 LKM - システム関数アドレスを自身の持つ関数アドレスに上書きする

- TCT：メモリ・ファイル状態をダンプする

事後対処

rootkit が検出された場合はサーバリストアを行う

- ・ システム再インストール
- ・ HDD イメージリストア
- ・ ネットワーク監視
 - IpLog、tcpdump、snort：ネットワークモニタとして利用する
 - ルータ、ファイアウォール、サーバのログチェック

事前対処

- ・ インシデント時システム停止基準の制定
- ・ ファイル改ざん検出ツールの導入
- ・ 正常ハッシュ値の保存
- ・ HDD イメージバックアップ
- ・ OS ブートイメージ作成：CD-ROM など
- ・ デュアルシステムの導入：サーバ可用性評価に基づく

まとめ

一般的な rootkit をそのまま利用するスクリプトキディレベルの侵入者の場合、既存の検知ツールは有効である。

カスタマイズ・新規作成された LKM によるシステム関数のつとりを被攻撃マシンで検出することは困難であり、rootkit が動作していない保証をすることは難しい。

LKM の対処を考慮したツール・手法は存在するが、理論上検知回避の可能性を否定できない。Windows も同様である。

正確な調査には汚染のないカーネル・コマンドが必要となる。これにはサービス停止を含めた運用体制が前提となる。

一般的な対策として 迅速なセキュリティホールの対策、FW、IDS など他のネットワーク機器によるセキュリティ確保が必要である。

さらなる防衛手段としては、ブート後の LKM 禁止 (LinuxKernel2.2 から)、よりセキュアなモデルの導入によるシステム関数監視があげられる。

詳細技術解説については、本サイトの不正アクセス手法検証結果を参照されたい。