A-1
「標的型攻撃と インシデントレスポンス」

文京学院短期大学
浜　正樹

基本概念

「インシデント」とは

- 組織が定めるセキュリティポリシーやコンピュータの利用規定に対する違反行為
- インシデント例
  - 不正アクセス、Webサイト改竄、DoS、情報窃取、コンピュータ侵入

「標的型攻撃」とは

- 特定の組織・個人の所有する機密情報の搾取を目的とするインシデントの1種
- 目的を達するまで、長期に渡って・何度でも攻撃する点が特徴

標的型攻撃に対する インシデントレスポンス

目標

- 標的型攻撃の確認
- 正確な情報収集の促進
- 対応戦略決定のための要因収集

方法論 [1]

1. 準備
2. 標的型攻撃の検出
3. 初期対応
4. 対応戦略の策定
5. 被害システムの複製
6. 被害・痕跡調査

方法論 [2]

7. セキュリティ対策の実施
8. ネットワーク監視
9. 復旧
10. 報告書の作成

初期対応の目的

- 被害の概要を把握
- 対応戦略決定のための要因収集

初期対応における確認事項

- 標的型攻撃の痕跡
- 被害を受けたシステム
- 関係しているユーザー
- 業務継続に与える影響

対応戦略の策定

- 攻撃者の活動監視
- 被害システムの分離
- システム復旧
- 漏洩情報の割り出し

対応戦略の決定

- 継続調査と被害システムの分離
- 専門機関への依頼
- 経営陣からの承認受諾

標的型攻撃被害調査

標的型攻撃の要素技術

- RAT
  - 遠隔操作ツール。標的型攻撃で悪用されることが多い
- Pass the Hash
  - Hash化されたパスワードを使いまわす手法

原因調査の項目(ネットワーク)

- 不審サイトへの通信ログ
- POSTメソッド
- 監査ログ(リモートログオン)

原因調査の項目(操作)

- 実行ファイルの特定
- スタートアップ登録状況
- タイムライン解析

MALWARE攻撃痕跡調査

調査ポイント (挙動を監視)

- 不自然な時間帯のファイル作成
- システム管理者用ツール等の利用痕跡
- USBメモリ等を介しての被害拡大

標的型攻撃に関連したファイル解析

解析対象ファイル

- 偽装ドキュメントファイル
- メモリダンプ
- 実行ファイルの動的解析
- ネットワークトラフィックファイル