標的型攻撃の実戦

2014/11/19

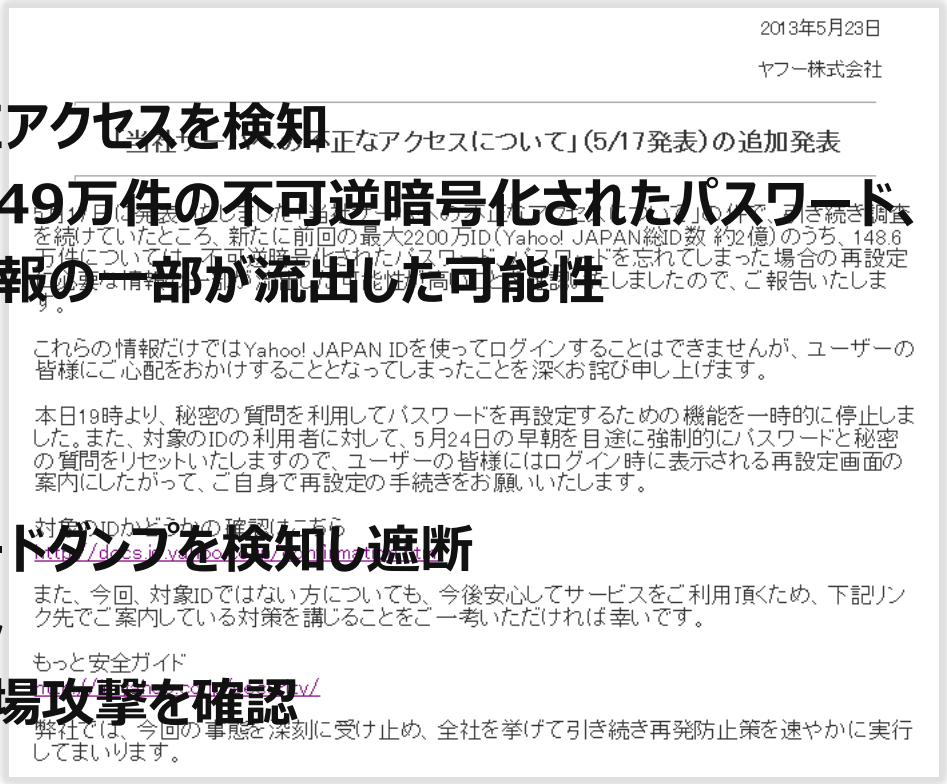
ヤフー株式会社
高　元伸

サイバー攻撃は現実の脅威

2013年ヤフーでの標的型攻撃

- **2013年4月**
  ポータルサイトを管理するシステムへの不正アクセス検知
  ユーザー情報の一部を抽出する不正プロセスを検知し遮断
  データの漏洩はなし

- **2013年5月**
  別手法でのシステムへの再度の不正アクセスを検知
  最大2,200万件のIDと、そのうち149万件の不可逆暗号化されたパスワード、
  およびパスワード再設定に必要な情報の一部が流出した可能性



2013年5月23日

ヤフー株式会社

「当社への不正なアクセスについて」(5/17発表)の追加発表

を続けていたところ、新たに前回の最大2200万ID(Yahoo! JAPAN総ID数 約2億)のうち、148.6
万件については、IDと不可逆暗号化されたパスワード、"ログインパスワード"を忘れてしまった場合の再設定
[illegible]しましたので、ご報告いたします。

これらの情報だけではYahoo! JAPAN IDを使ってログインすることはできませんが、ユーザーの皆様にご心配をおかけすることとなってしまったことを深くお詫び申し上げます。

本日19時より、秘密の質問を利用してパスワードを再設定するための機能を一時的に停止しました。また、対象のIDの利用者に対して、5月24日の早朝を目途に強制的にパスワードと秘密の質問をリセットいたしますので、ユーザーの皆様にはログイン時に表示される再設定画面の案内にしたがって、ご自身で再設定の手続きをお願いいたします。

対象のIDかどうかの確認はこちら

また、今回、対象IDではない方についても、今後安心してサービスをご利用頂くため、下記リンク先でご案内している対策を講じることをご一考いただければ幸いです。

もっと安全ガイド

弊社では、今回の事態を深刻に受け止め、全社を挙げて引き続き再発防止策を速やかに実行してまいります。

- **2013年10月**
  ゼロデイ攻撃を検知
  社内用の管理サーバ上でのパスワードダンプを検知し遮断
  サービスおよびユーザーへの影響なし
  分析の結果マルウェア感染と水のみ場攻撃を確認

事例：社内ネットワークへの侵入

投影資料を参照ください

振り返り ～ 最悪のケースは

- 業務端末への侵入
- 重要エリアへの侵入調査
- システム管理者の権限奪取
- **ID管理DBへ侵入**
- 情報流出と痕跡消去
- 顧客アカウントへの不正侵入
- 被害を認識した顧客からの問い合わせ
- 不正アクセス確認と詳細調査困難との報告
- 記者会見

攻撃の存在を察知する
侵入に対する時間を稼ぐ
攻撃を遮断する
影響範囲を確認する

通常とは異なる兆候への意識

マルウェア検知
システム負荷
予測しないプロセス
作業申請時間外のログイン
申請内容とは異なるサーバへの接続
想定以上のリクエスト

相手もインテリジェンスを持っている

変化の兆候に気づく
一見正常でも頻度の変化に異常がある

自然災害とは異なる
設計の想定外の手法を意図的に選択してくる

マーフィーの法則…ではない
ルールと運用のギャップが狙われる

短期に実施したこと

対応方針の確認

影響範囲の確認

再侵入防止

マルウェア対策

広報・CS対応

二次被害防止

フォレンジック

社内意識の啓発

対策方針と課題確認

ユーザーファースト

各種ログ監視体制の強化

サーバ認証強化

検知ソリューションの導入

判定ツールの提供

ユーザへの注意喚起

外部専門会社への支援要請

社内ポータル・研修・実施報告

経営陣を含めた振り返り合宿

侵入防止
攻撃検知
事故対応

対策の考慮点

単一のソリューションでは対処し得ない

テクニカルソリューションだけに偏らない

技術部門の対策が全てではない

発生を防ぐことだけにこだわらない

システムと情報の配置
運用人員体制

攻撃の標的	認証・信用情報・名簿・技術情報
標的の価値	量の優位性・価値の希少性
攻撃の目的	金銭・思想・誇示・企業競争・軍事

情報価値と影響の認識

システムと情報配置の把握

権限とアクセス経路の棚下ろし

運用手順と承認フローの確認

現状の固有リスクは何か

ヤフーの持つユーザ情報と基盤

YAHOO! JAPAN

PCI DSS COMPLIANCE

利用者

※7,354万ユニークブラウザ/日

2,829万ID 月間アクティブユーザー

※2014年7-9月現在
Yahoo! JAPANサービスを閲覧するために利用されたブラウザ数

決済

YAHOO! JAPAN ウォレット

2,700万人

※2014年9月現在

防御は不利か？

防御　(Wikipedia抜粋)

敵の攻勢作戦を妨げ、時間的な猶予を獲得し、
ある地域への接近を拒否し、攻撃力を減退させる効果

戦術上は防御側が有利

- システム構成の熟知
- ログイン経路の遮断・制限
- サービス停止の選択肢

攻撃者の利点

- 攻撃対象・タイミングの選択
- ゼロデイ等の攻撃秘匿性

個々の対策に何を期待する？

マルウェア検知

パスワード認証

情報分析ソリューション

痕跡の分析

脆弱性情報への対処

対策の鮮度も重視
攻撃相手も有効性を評価している
全てに万能な対策はない
作業負荷軽減と効率化

対策ツール以上に人的対応

攻撃手法は常に“初めて”

攻撃の動きに応じた対応

効率を上げるためのツール

発生時の対応

インシデントレスポンスチーム
システム担当者
監視運用
経営層
サービス責任者
広報・CS・法務
人事・総務
ツール開発担当者

発生検知

異常検知
判断と初動対応
エスカレーション
緊急事態宣言

初期対応

被害拡大防止
影響範囲特定
原因分析
対応方針決定
対応人員補給入替

事態収拾

情報開示
顧客対応
再発防止
顧客フォロー
課題振り返り
効果確認

各フェイズで時間軸、中心となる人員が異なる
事故発生回避以上に二次被害発生回避
顧客対応の方針でレピュテーションリスクは大きく変わる

対応のポイントは

迅速なエスカレーションと迅速な決断

リソース投入を惜しまない

適切な情報開示とタイミング

初動の明確な対応指針

現場への適切な権限委譲

事実事象の把握

時系列での整理

最悪のケースを想定した防衛ライン

案件対応責任者
意志決定者
時系列記録者
対応支援者

乗り越えるべき課題

チームプレイはできているか

死守するものは何か

User First

顧客の利益と企業への信頼

地道な継続

保有情報と権限の棚卸し

検知アラートとログの分析

重要情報の再配置

監視と運用体制の是正

セキュリティ教育と啓蒙

攻撃者視点の監査

セキュリティ犯罪の動向・事例
各種脆弱性情報・注意喚起の注視

完封勝ちを目指さない
エラーは なるべく しない
ファインプレーを期待しない
点を取られても試合には勝つ

ご清聴ありがとうございました

※本資料に使用しているデータの二次利用はご遠慮ください