2019 年 8 月 27 日

サービス＆セキュリティ株式会社 e-Gate センター

パスワードクラッキングの手法と対策について

1. 概要

「パスワードクラッキング」とはシステムへのログインや特定機能を利用する際に利用者が本人であるかを確認するためのパスワードを割り出し、不正にログインする攻撃です。

多くのサービスで広く一般的に使われているパスワード認証ですが、パスワードを知らないはずの第三者に認証を突破され、不正利用の被害に遭ってしまったという事例は後を絶ちません。

8 月 7 日に IPA より公開された「情報セキュリティ 10 大脅威 2019」においても直接または間接的にパスワードクラッキングが関係している脅威が多数ランクインしており、8 月 8 日(米国時間)にはオーストラリアのサイバーセキュリティセンター(ACSC)よりパスワードクラッキングの手法の一つである「パスワードスプレー攻撃」がオーストラリアの組織を対象に行われたことを観測したとの情報が公開されています。

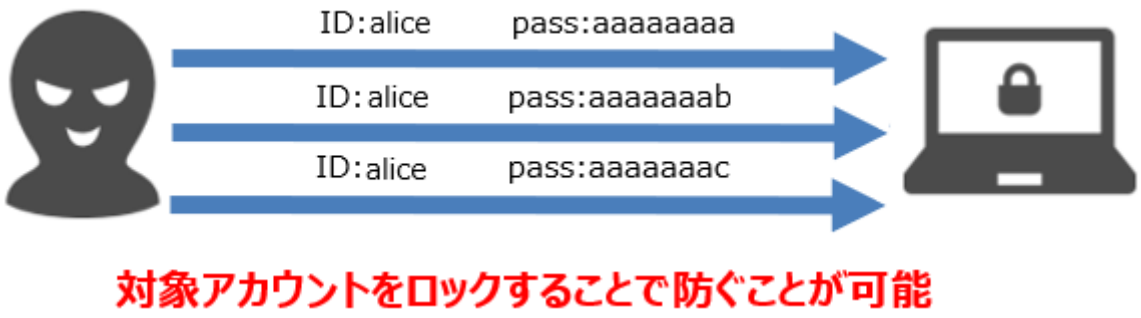
DX(デジタルトランスフォーメーション)によって企業の取り組みや人々の生活においてあらゆることがデジタル化されつつあり、そうした流れの中で攻撃対象の増加・技術の高度化に伴い攻撃の増加・巧妙化が予測されます。

以降、パスワードクラッキングの手法とその対策についてご紹介致しますので、セキュリティ対策にご活用ください。

2. 攻撃手法

■ブルートフォース攻撃

「総当たり攻撃」とも呼ばれる攻撃手法で、図 1 のように特定の ID に対してパスワードとして使用可能なすべての文字列を組み合わせてログインを試みます。単純な原理で実施も容易であり、時間さえかければ確実に認証の突破が可能となる強力な攻撃手法です。



【図 1：ブルートフォース攻撃のイメージ】

■辞書攻撃

人名や辞書に載っている英単語など、覚えやすい意味のある文字列を用いてログインを試みます。試行対象の文字列には単語の一部を大文字にしたものや数字・記号を付加したものも含まれています。

■パスワードリスト攻撃

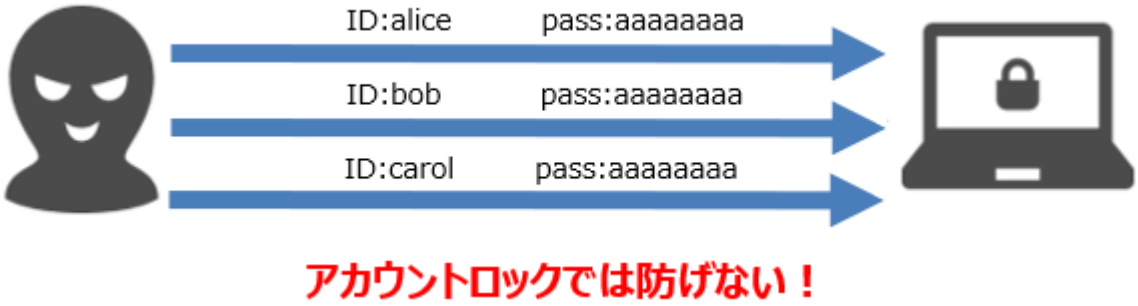
攻撃者が別の手段で事前に入手してリスト化した ID とパスワードの組み合わせを利用してログインを試みます。複数のサービスで同じ ID とパスワードを使い回したり、推測されやすい文字列を使用したりすると攻撃を受けるリスクが高まります。

■リバースブルートフォース攻撃

通常のブルートフォース攻撃では特定の ID に対してすべてのパスワードを試行するのに対し、リバースブルートフォース攻撃では図 2 のように特定のパスワードを複数の ID に対して用いてログインを試みます。

特定の ID に連続してログインを試みないので、パスワードクラッキングへの防御策として広く用いられているアカウントロックを回避することが大きな特徴です。また、辞書攻撃やパスワードリスト攻撃と併用される場合が多いといわれています。最近では送信元 IP アドレスを変化させつつ、複数のサービスへ一定の時間を置きながら試行を繰り返すなど検知を難しくするための工夫がなされていることもあり、そうした時間をかけてゆっくりと認証の突破を試みる手口は「パスワードスプレー攻撃」「low-and-slow 攻撃」などと呼ばれます。

徹底して痕跡を隠されると入力ミスなどによる正規ユーザの認証失敗と攻撃者による認証失敗を見分けることが難しく、実際に 2018 年 10 月から 2019 年 3 月にかけて大手 IT 企業の C 社を対象にこの攻撃が行われ、不正アクセスを許してしまったとされる事例もあり、検知することの難しさが伺えます。



【図 2：リバースブルートフォース攻撃のイメージ】

■パスワード窃取

それぞれの詳細な手法については割愛しますが、以下のような手段でパスワードを窃取し、その情報を用いて不正ログインを試みます。窃取された情報がハッシュ化されていた場合も、平文とハッシュ値の対応表であるレインボーテーブルを事前に用意して突き合わせることで平文のパスワードを解析されてしまう恐れがあります。

【パスワード窃取の手法】

① フィッシング
② システムの脆弱性を突く
③ マルウェアやキーロガーを仕込む
④ ショルダーハック

3. ユーザ側での対策

■意味を持たず、できるだけ長いパスワードを設定する

パスワードクラッキングは総当たりや推測によってパスワードを割り出そうとするものが多く、短いパスワードや意味のある文字列では攻撃を受けるリスクが高まります。

最近では使用する文字数を極端に多くした「パスフレーズ」を利用するケースもあります。これは単に総当たりに要する時間を長引かせるだけでなく、覚えやすい意味のある文字列を設定した場合にも複数の単語を組み合わせる必要があり、大文字小文字の違い・数字や記号の付加なども考慮すると膨大な数のパターンが存在し得るため、辞書攻撃によるパスワードクラッキングを困難にするという効果もあります。

■複数のサービスで同じパスワードを使いまわさない

複数のサービスで同じパスワードを使いまわした場合、一つのサービスからパスワードが漏洩した際に、パスワードリスト攻撃によって他のサービスにまで不正利用の被害が及んでしまいます。

異なるパスワードを管理する手間や忘却のリスクとトレードオフではありますが、複数のパスワードをまとめて管理するためのツールも存在しており、これを利用することで容易に実現が可能です。但し、パスワード管理ツール自体の管理や取り扱いは厳格にする必要があります。

■使用端末の OS やセキュリティソフトの状態を最新に保つ

マルウェアに感染してパスワード情報が漏洩することを防ぎます。パスワードクラッキングへの対策に限らずセキュリティを向上させる上で重要な対策です。この対策はシステム管理者側にも求められます。

■人目の多い場所でログイン操作を行わない

人目の多い場所では、ログイン操作を行う際の画面表示・キーボード操作や画面タップ操作などを盗み見ることでパスワードを窃取するショルダーハックのリスクが高まります。どれほど強固なパスワードでも他者に知られてしまうと役に立たないため、入力操作を行う際にも注意が必要です。

■利用サービスを選択する際はセキュリティ面にも意識を向ける

システムの脆弱性を突いてパスワードを窃取された場合、ユーザ側で防ぐ手立てはありません。

本来、そうした事態を防ぐ責任はサービスの提供元にありますが、実際に被害を受けるのはユーザであり、サービスの提供元が被害のすべてを補填してくれるとは限りませんし、個人情報の流出など取り返しのつかない被害も起こり得ます。

数ある類似サービスの中から利用サービスを選択する際、どうしても価格やサービス内容ばかりに意識が向いてしまいますが、以下のようにセキュリティ面や万一に備えた補償の有無に少しだけでも意識を向けることが被害の防止に繋がります。

【意識を向けるべき点】

① 多要素認証や多段階認証が利用可能か
② https を利用しているか
③ ID やパスワードを忘却した際の初期化手続きはどのように行われるか
④ 不正アクセスによる被害に対する補償が規約に盛り込まれているか

4. システム管理者側の対策

■アカウントごとのログイン試行回数に上限を設ける

規定回数以上認証に失敗した場合はアカウントを一定期間使用不可能にする機能を実装することで、特定のアカウントに対する総当たりでのパスワードクラッキングを防ぐことが可能です。

■危険なパスワード設定時にユーザへ警告を行う

短すぎる、文字種が少ない、パスワードとして設定されやすい文字列などの類推されやすいパスワードが設定された場合、警告を表示して再設定を促す機能を実装することで、危険なパスワードの利用を防ぐことが可能です。

■サーバなどで保持する認証情報は平文のまま保存しない

攻撃者からサーバなどに保存された ID・パスワードが窃取された際、平文のまま保存されていた場合は直ちに不正ログインの被害へと繋がるため、対策としてハッシュ化にて平文の特定を困難にすることが有効です。

また、その際は先述したレインボーテーブルへの対策として、ハッシュ化前の平文にユーザごとに異なるソルトと呼ばれる文字列を付加する方法とハッシュ化で求めた値を更にハッシュ化する処理を複数回繰り返すストレッチングの実装が求められます。

これらの対策は独自の方法で実装すると脆弱性が混入する恐れがあるため、使用する言語ごとに推奨されている専用のハッシュ関数を利用して実装する必要があります。

■多要素認証・多段階認証を実装する

SMS 認証や生体認証など、別の認証方法との併用や、以下のような点が普段と異なる環境からログインが行われた際に追加認証を行うリスクベース認証を実装することで、パスワード認証を突破された場合にも被害の発生を防ぐことが可能です。

【リスクベース認証の判断材料】

① IP アドレス
② 端末情報
③ 使用 OS
④ ISP
⑤ 位置情報

■ログインの試行を記録して怪しい動きがないか監視する

パスワードクラッキングが行われる場合、以下のように特徴的な記録が見られます。それらの情報を発見し、ユーザへ通知を行ったり、IP アドレスを基に通信を遮断したりするなど適切な対処を行うことで被害を抑えることが可能です。

これを実現するために、セキュリティ機器や監視基盤を導入し、SOC にてログインの試行状況を監視することが有効です。

【パスワードクラッキング時に見られる特徴】

① 特定の IP アドレスから大量のログイン試行
② 存在しない多数の ID へのログイン試行
③ 普段と異なる環境からのログイン

5. e-Gate の監視サービスについて

Firewall や IPS をはじめとするセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。“e-Gate”の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

6. 参考情報

IPA(独立行政法人 情報処理推進機構)

- 情報セキュリティ 10 大脅威 2019
  https://www.ipa.go.jp/security/vuln/10threats2019.html

- 不正ログイン対策特集ページ
  https://www.ipa.go.jp/security/anshin/account_security.html

JPCERT

- 適切なパスワードの設定・管理方法について
  https://www.jpcert.or.jp/newsflash/2018040401.html

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp