2021 年 01 月 26 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：ブルートフォース攻撃の増加状況と対策について

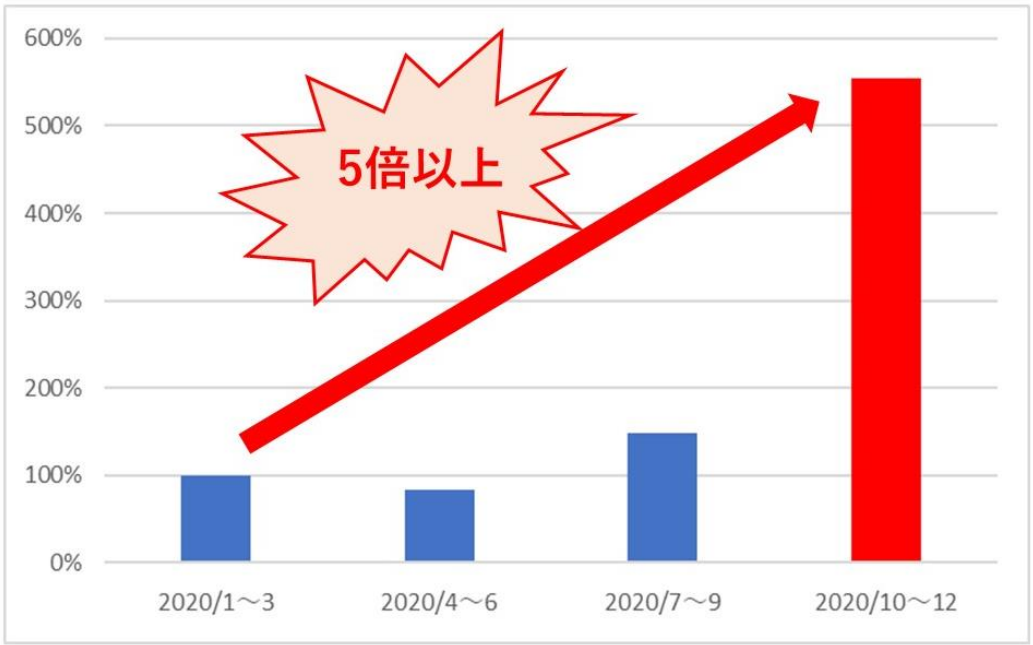
1. 概要

近年複雑で様々な手口の攻撃手法が開発されておりますが、古くから攻撃者に使用されている攻撃手法にブルートフォース攻撃があります。当該の攻撃は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。現在でも使用され続けており、ここ数ヶ月で e-Gate センターでも検知数の急増が確認されております。今回は、今なお使用され続けるブルートフォース攻撃について、その特徴と対策をご紹介いたします。本記事をご参考いただき組織内での対策がなされているか今一度ご確認いただくことを推奨いたします。

2. e-Gate センターにおけるブルートフォース攻撃検知の推移

前述の通り e-Gate センターでもブルートフォース攻撃イベントは増加傾向にあります。今年の 9 月までと比較して、10 月から検知数が大幅に増加しており今後も増加する可能性が考えられます。

2020 年 8 月に発生した VPN 認証情報の流出事件があったように、テレワークの増加に伴い認証情報流出のリスクは高まる可能性があります。攻撃者は入手した ID などの情報をもとにブルートフォース攻撃などを用いたさらなる不正アクセスを試みているものと見られます。このような攻撃により社内へ不正なアクセスをされてしまった場合、機密情報を窃取される危険性が増大します。



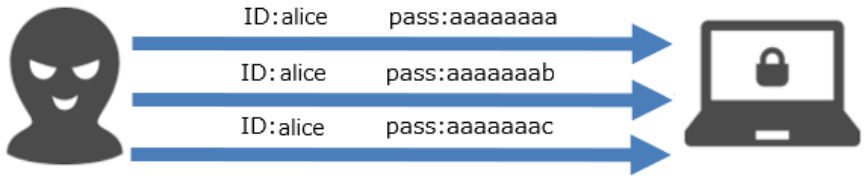
【図 1】e-Gate センターにおけるブルートフォース攻撃イベント数の推移（2020 年 1～3 月を 100%として算出）

3. ブルートフォース攻撃とは

ブルートフォース攻撃とは、パスワードのすべての組み合わせを試し、不正ログイン等を行う攻撃手法です。ブルートフォース攻撃と、ブルートフォース攻撃に類する攻撃を紹介します。

■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、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。



【図 2】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。

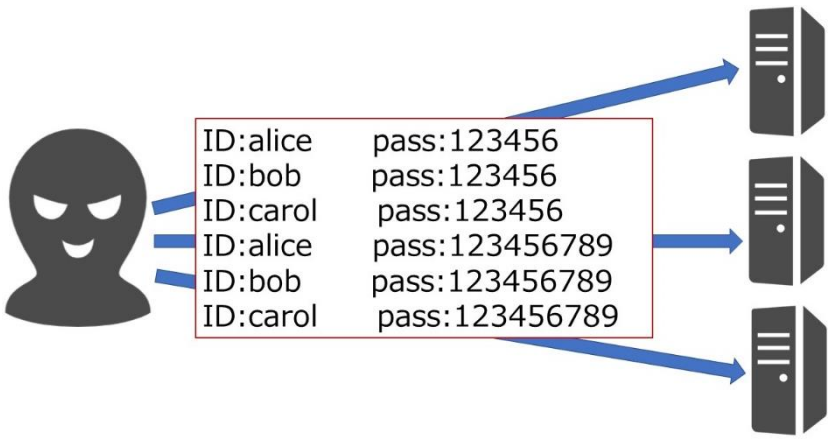
■リバースブルートフォース攻撃

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。

リバースブルートフォース攻撃の一種である「**パスワードスプレー攻撃**」は、不正アクセスの検知を回避する可能性のある攻撃手法です。「low-and-slow 攻撃」とも呼ばれるこの攻撃は、リバースブルートフォース攻撃の中で送信元 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します。

短時間で同一 ID に対し大量のログインを試みる通常のブルートフォース攻撃と比較して、正規ユーザの認証失敗と攻撃者による認証失敗の判別が難しくなり、不正アクセスの検知を回避する可能性が高くなることが特徴です。

平易なパスワードを使用しているユーザが多いサービスの場合、多数のユーザが不正アクセスの対象となり、ユーザ情報流出の原因となるリスクが高まります。



【図 3】パスワードスプレー攻撃のイメージ

4. ブルートフォース攻撃によるマルウェア感染拡大の危険性

ブルートフォース攻撃はポートスキャンやフィッシング等、様々な攻撃と組み合わせて用いられることが多くなっています。また、ブルートフォース攻撃を用いたマルウェア感染展開活動も確認されています。

「Kaiji」は DDoS（分散型サービス妨害）実行を目的としマルウェアで、SSH や Telnet のポートスキャンを行った後に、ボット型マルウェアでブルートフォース攻撃を実行し感染を広げます。トレンドマイクロによると、最近は Docker API で使用する 2375 番ポートに対するスキャン活動が見られたとされており、Docker サーバに対し感染拡大の危険性が考えられます。

また、マルウェア「Stealthworker」は cPanel / WHM、WordPress、Drupal、Joomla、OpenCart、Magento、MySQL、PostgreSQL、Brixt、SSH、FTP などに対してブルートフォース攻撃の実行が可能で、バックアップファイルや管理者のログインパスの検索なども行います。国内シェア数の多い WordPress なども対象となっており、注意が必要です。

5. ブルートフォース攻撃の対策

【ユーザ側での対策】

ユーザ側では利便性を優先するため平易なパスワードを設定しがちです。しかし、被害にあった際のリスクを考え、ひとりひとりの IT リテラシを向上させることがもっとも重要な対策と言えます。そのうえで以下のような対策をとることを推奨いたします。

- 複雑なパスワードを設定する

  現在は攻撃用のツールも進化しており、前述のようなよく使われるパスワードを設定した場合、1 秒未満～数秒でクラッキングされる可能性があります。大文字・小文字・数字や記号を組み合わせ、できるだけ長いパスワードを設定することで安全性が大きくに向上します。ブルートフォース攻撃に要する時間を長引かせることができ、システムの管理者側での攻撃の検知にもつながります。またパスワードリスト攻撃などの攻撃を避けるため、意味のある文字列を避けることも有効な対策です。

- 同じパスワードを使いまわさない

  同一のパスワードを複数のサービスで使いまわした場合、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。パスワード管理ツールを適切に利用するなど、利便性とのバランスも考え、対策することが有効です。

- 利用するサービスのセキュリティを意識する

  多要素認証に対応しているか、https を利用しているか等、利用するサービス選択の際、サービス内容以外にセキュリティ面に対する確認を行うような意識を持つことが重要です。

【システム管理者側での対策】

システム管理者とユーザ間では、セキュリティに対する意識の相違が生まれがちです。そのことを念頭において幅広い視野で対策を講じることが重要です。以下の項目を参考に今一度、組織内での対策がなされているかご確認いただくことを推奨いたします。

- 平易なパスワード設定に対する制限を行う

  一定文字数以上、複数の文字種混合させたパスワード設定を要求する等、平易なパスワード設定に対する制限を設ける事でユーザが危険なパスワードを利用するリスクを低減することが可能です。また利便性を考え、平易なパスワー

ドに対し警告を表示するにとどめる等、サービスの種類によりセキュリティと利便性のバランスを考えることも重要です。

●ログイン試行回数に制限を設ける

ログイン試行回数に制限を設け、規定回数以上ログインに失敗した場合に再入力まで一定時間アカウントをロックするよう制限することでブルートフォース攻撃に対するリスクを大きく減少させることができます。

●多要素認証（多段階認証）を実装する

メールを利用したワンタイムパスワードによる二段階認証や、生体認証等の導入はブルートフォース攻撃に対し特に有効な対策です。ユーザの利便性を考慮しつつ、サービスの種類によって導入の有無を検討することが重要です。

●セキュリティ機器で攻撃通信を監視する

セキュリティ機器を導入することで、ブルートフォース攻撃などの攻撃通信を監視します。攻撃通信を検知した場合、攻撃元の情報をもとに通信の遮断や、ユーザに対する通知を行う等の対処が可能です。セキュリティ機器の適切な運用にはセキュリティベンダを利用することも有効です。

6. 参考情報

・TrendMicro

2 種の Linux ボットで露出した Docker サーバを狙う活動を確認：「XORDDoS」と「Kaiji」

https://blog.trendmicro.co.jp/archives/25946

・Akamai

STEALTHWORKER: GOLANG-BASED BRUTE FORCE MALWARE STILL AN ACTIVE THREAT

https://blogs.akamai.com/sitr/2020/06/stealthworker-golang-based-brute-force-malware-still-an-active-threat.html

7. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策として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い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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」と最新のメソッドで構築した「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”サービスです。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/

«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