2022 年 1 月 27 日
ラシン株式会社

弊社サーバの不正アクセス被害についてお詫びとご報告

この度、弊社サーバが第三者からの不正アクセスの被害に遭い、管理しているサイトの掲載を一時止めて原因の究明に努めて参りました。
お客様や関係者の皆様に多大なるご迷惑とお心配をおかけした事、深くお詫び申し上げます。
本件に関して経緯と原因、また今後の対策に関して以下の通りご報告申し上げます。
今後は更なるセキュリティ強化に努めると共に、再発防止に向け徹底して取り組んで参ります。

1. 被害判明に至る詳細経緯

2021 年 12 月 6 日、弊社契約のサーバ会社から連絡があり、弊社管理のサーバが著しく高い負荷状態であることから、サーバ会社により、弊社管理の全てのサイトに対して強制的にアクセス不可とする安全措置をとった旨の連絡がありました。

弊社のサーバのアクセスログには、弊社のサーバ自身を示す IP アドレスから不審な操作を行っているログがあり、弊社で使用する CMS を使った不正アクセスの可能性、更にはサーバそのものに不正アクセスがあった可能性から、悪意ある攻撃者によって何らかのセキュリティ侵害が行われた可能性が高いと判断し、その被害範囲の特定と原因究明の為、アスエイト・アドバイザリー株式会社に依頼し、デジタル・フォレンジック調査を実施いたしました。

2. 調査結果

調査の結果、本件被害の端緒は、「CMS の管理画面への不正ログイン」であることが判明いたしました。

この原因は、CMS におけるセキュリティ対策が不十分であった為に管理者アカウントが攻撃者に取得されたことによるもので、攻撃者は不正ログインに成功した後、Web Shell を設置して、サーバ内のディレクトリ情報を収集した上で、更に複数のディレクトリに Web Shell やファイルアップロードプログラムの設置を行ったと推測されます。

今回の不正アクセスによって行われた攻撃は、下記と推測されます。

- CMS の管理画面への不正ログイン
- ブラウザを使用して Web 経由でサーバ上のコマンドの実行やファイルの編集、アップロードなどユーザの実行権限の範囲でサーバをコントロールすることを可能にする不正なプログラム「Web Shell」の設置
- ファイルをアップロードすることができるプログラムの設置
- 侵害を行った Web サイトの情報を Google 検索で調べた際に、検索結果の上位に攻撃者が用意した不正なサイトを表示するようにする「SEO Spam」の設置
- 攻撃者が意図的にフィッシングメールやスパムメールを送信することを目的とした、PHP で作成されたメールクライアントプログラムの設置
- Web Shell プログラムを実行させるために、ディレクトリ単位で Web サーバの設定を制御するサーバ設定情報 の改ざん

3. 被害範囲

Web Shell が設置された時点で、攻撃者によってファイルの作成、編集、削除、アップロード、そしてデータベースの参照が行える状態になっており、事実、調査を開始した 2021 年 12 月 10 日 10 時の時点で、234 種類に及ぶ全 65,959 もの不正ファイルがサーバの複数のディレクトリに設置されていたことが判明いたしました。

しかし、サーバ上のアクセスが行われているファイル名やアクセスログを調査した結果、送信データサイズが 1MB 以上のデータを送信した形跡がないこと等から、機微な情報をふくめたデータベースのダンプやサイト全体のバックアップを攻撃者によって収集された可能性は極めて低いと推測されます。

これらの状況から確認された被害は下記となります。

- Web コンテンツを構成するファイルの改ざん
- 検索エンジンへの登録情報の改ざん
- サーバの弊社管理領域に対するセキュリティ侵害

4. 再発防止策

今回、被害にあったセキュリティ侵害と同種のサイバー攻撃を防ぐには、今後、適切なシステム運用及びセキュリティ対策を行うことで、被害を未然に防ぐことが可能と考えます。

また、日々巧妙化するサイバー攻撃対しても常に最新の知識と対策を得らえるよう専任のアドバイザーを設置し、セキュリティ体制の強化と予防対策を実施してまいります。

具体的予防策として以下を実施いたします。

I. 各種プログラム・プラグインを常に最新の状態に保つためのアップデートの実施

II.　不要機能の無効化・削除と確認頻繁化のためのルール作り
III.　アクセス権限の管理と制限の確実な実施
IV.　URL のセキュリティ性の向上
V.　識別子複雑化等のブルートフォースアタック対策の実施
VI.　強固な Web Application Firewall（WAF）の導入
VII. 第三者機関のセキュリティアドバイザーの設置
VIII. スケジューリングによる第三者機関からのセキュリティ診断の実施
IX.　第三者機関を交えての月次セキュリティリスクアセスメントの実施

＜本件に関するお問い合わせ先＞

ラシン株式会社：担当　道原（ミチハラ）
TEL：092-725-5708（受付時間：午前 9 時 30 分～午後 6 時 30 分）
E-mail：bariyoka-customer@rashin.jp