2022 年 09 月 24 日

サービス＆セキュリティ株式会社 e-Gate センター

脆弱性スキャンツール「ZGrab」を悪用した攻撃と対策について

1. 概要

弊社セキュリティオペレーションセンター（SOC）である e-Gate センターにて直近 1 年間に検知数がおよそ 2 倍となっている攻撃があります。脆弱性スキャンツール「ZGrab」に関する攻撃です。ZGrab は脆弱性をスキャンすることで、企業のセキュリティなどを調査し強化することを目的としています。しかし、攻撃者によってスキャンが行われ一度脆弱性が見つかると、その種類に応じた攻撃が行われます。

今回は ZGrab を悪用した攻撃の手法と対策について紹介いたします。

2. ZGrab とは

ZGrab は、大規模なインターネットの調査をするために設計されたアプリケーション層ネットワークスキャナー（※1）です。パブリックインターネットを構成するホストとサービスの大規模な実証分析を行うために、オープンソースツールやライブラリを集約したコレクション「ZMap Project」の内の一つです。ZGrab は、インターネット全体のネットワーク調査用に設計された「ZMap」と組み合わせて使用されることが多く、OSINT ツール（※2）の SHODAN や Censys の情報更新にも利用されています。また、企業においては運用中のサービスに対して脆弱性を点検するツールとして使用されます。

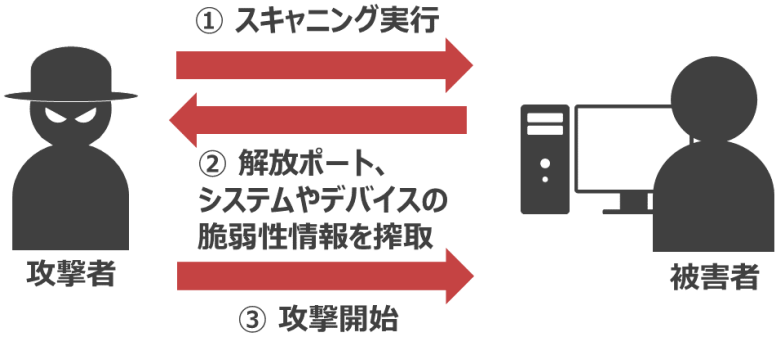
オープンソースツールであるため誰でも利用できるという点が特徴ですが、反面、攻撃者によって悪用される危険性もあります。モジュール式で処理能力が高速の為、攻撃者がツールを利用しやすく、大量の攻撃も可能です。攻撃者は悪用を目的としてスキャンを実行し脆弱性を検出すると、その対象のポートに脆弱性の種類に応じた攻撃を行います。

下記は、ZGrab を悪用し攻撃に至るまでの流れになります。（Web アプリケーションサーバの例となります。）

① 攻撃者が ZGrab を用いて、被害者の web アプリケーションサーバにスキャニングを行います。

② 攻撃者はスキャニングによってポートの解放状態を確認します。解放ポートからさらに、システムやデバイスなどの脆弱性をスキャンし、Web アプリケーションに脆弱性があることを見つけ出します。

③ 攻撃者は脆弱性が判明した複数の Web アプリケーションサーバの中から、特定のサーバに対して Web アプリケーションの脆弱性を突いた攻撃をはじめます。



【図 1】攻撃の仕組み

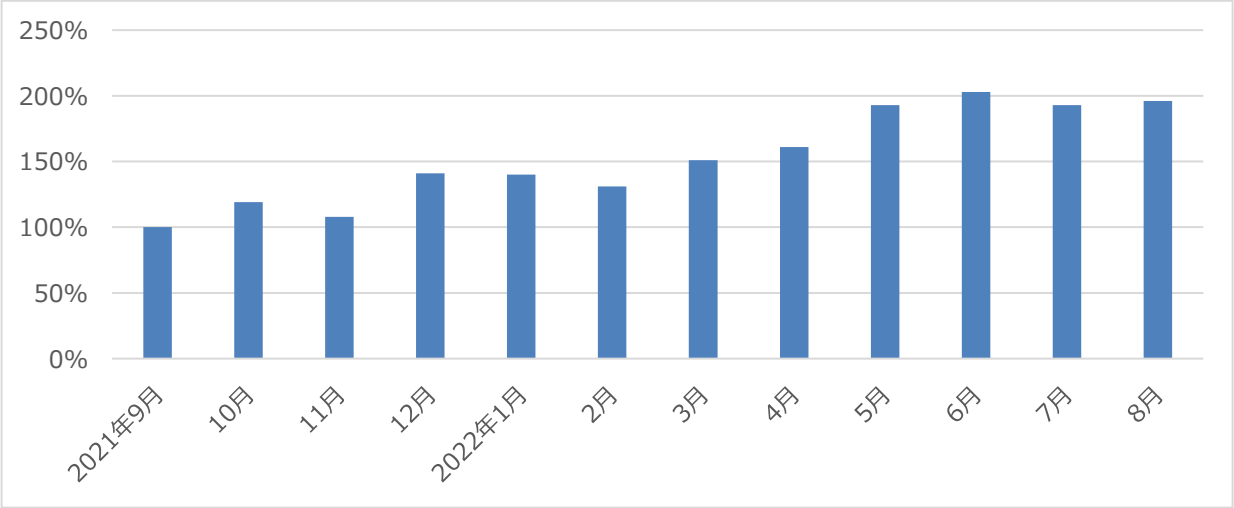
例として Web アプリケーションの脆弱性がある場合を挙げましたが、攻撃の段階からは SQL インジェクション、クロスサイトスクリプティング、ディレクトリトラバーサルなどあらゆる攻撃が考えられます。その他の通信ポートでの脆弱性が発見された場合のサーバへの侵入などが考えられます。

※1：ネットワークスキャナーとは、ネットワークを利用する全てのデバイスに対して脆弱性がないかスキャンをするツールのことです。

※2：OSINT とは、Open Source Intelligence（オープンソースインテリジェンス）の略であり、セキュリティ分野では一般的に公開されている情報からアクセス可能なデータを収集し分析することでサイバー攻撃の特定を行うことです。OSINT ツールは、データ収集時に用います。

3. e-Gate センターにおける攻撃検知

e-Gate センターでは ZGrab を悪用した攻撃を継続的に検知しています。下図は 2021 年 9 月以降の ZGrab 関連イベントの検知数の推移です。徐々に ZGrab を悪用した攻撃が増加しており、2022 年 5 月以降は 12,000 件を超える攻撃が毎月行われています。



【図 2】e-Gate センターにおける ZGrab 関連イベント数の推移（2021 年 9 月度を 100%として算出）

4. 対策

ZGrab 関連の攻撃への対策として以下の方法があります。

・ポートの管理

未使用のポートを閉塞しておくことにより、不審な通信をシャットアウトできます。

・User-Agent フィールドに対する検査の実施

Web アプリケーションサーバを運用している場合は HTTP 通信ヘッダの”User-Agent フィールド”に対する検査を実施することにより、脆弱性を取り除きます。

1. 特殊文字などは置換して処理します。
2. 正常な値のみ許容します。

・最新バージョンのアップデート適用

アプリケーションやソフトウェア、OS の開発元より公開されている脆弱性を修正したバージョンへのアップデートが推奨されます。

・セキュリティ機器による攻撃通信の監視

Firewall や IPS（侵入防御システム）等のセキュリティ機器により、不審な通信を検知・遮断することも一定の効果が見込めます。

ZGrab はあくまで脆弱性の有無を確認するツールでしかありません。しかし、e-Gate センターにおける検知数の増加傾向からしてもこのようなツールを悪用した攻撃が増加する一方です。常日頃、脆弱性を取り除きつつ、攻撃を受けているのか監視により可視化するなどの基本的な対策を取ることが安全なネットワーク環境の維持運用、改善に繋がります。

5. 参考情報

・ZGrab

zmap / zgrab2

https://github.com/zmap/zgrab2

脆弱性スキャンツールの悪用について

https://www.mcsecurity.co.jp/?page_id=3977

ZGrab.Scanner

https://www.fortiguard.com/encyclopedia/ips/48805

・ZMap プロジェクト

The ZMap Project

https://zmap.io/

・攻撃を目的としたスキャンに備えて 2019 年 7 月

https://www.jpcert.or.jp/newsflash/2019072201.html

6. 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