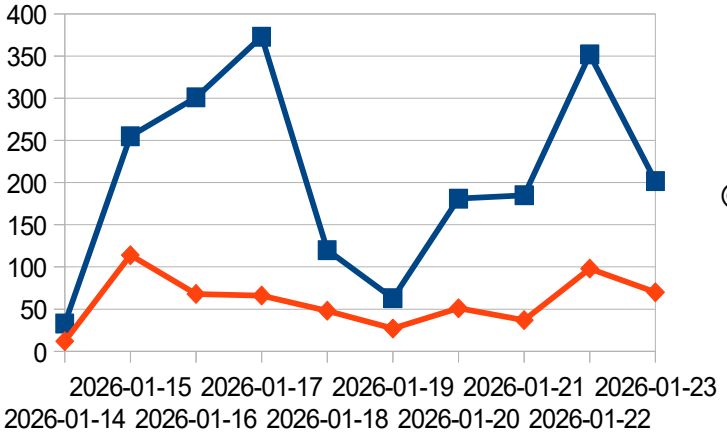
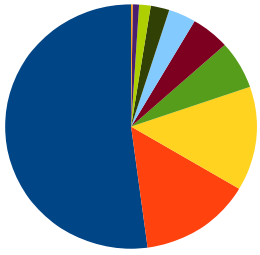
Honeypotレポート(20260114～20260123)

ハニーポットサーバ１台（解放ポート80,8080）に対するリクエストを解析し、結果をまとめました。

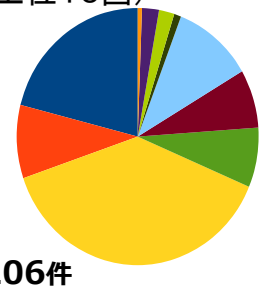
◎I-1　リクエスト回数の推移（日毎）



◎I-2 リクエストの割合（上位10国）



◎I-3 攻撃リクエストの割合（上位10国）



※　補足

総アクセス数　2066件、総攻撃数　591件、**一日平均　約206件**

国の識別はIPアドレスからGeolite2のcountry_iso_codeを使用して集計

◎ 攻撃の特徴

今回最も狙われていたのは、Next.jsに対するプロトタイプ汚染を使ったものが多く観測されました。次点は、APACHEのCGI-BINに対するパストラバーサル攻撃でした。

これらのでは、脆弱性を使用して、

ncコマンドによるバックドアの開設

wgetコマンドによる不正プログラムのダウンロード

を目的としていました。

今回観測した攻撃は、修正パッチがでている脆弱性を使用したものばかりでしたので、適切なアップデートと適切な権限設定を行っていれば防ぐことが可能です。

◎ 感想

家庭用ルータのポートを１０日間開いただけで、これだけの攻撃を観測することができました。攻撃者は総当たりで脆弱性を検索していますので、インターネット機器（特にルータ）は、確実なバージョンアップを行う必要があると改めて感じました。

ポート解放した時は、**開始からわずか１０分でプロトタイプ汚染のRCEが送られていました**ので、短時間であっても、古いルータをインターネットに接続するのはやめましょう。

今期に観測した攻撃の説明

●CMD_INJECTION
リクエスト内に wget, curl, tftp, nc, bash, sh などの OSコマンドを含み、サーバ上での実行を狙う リクエスト

●PATH_TRAVERSAL
「../」や複合することでこれと同じ意味を有する文字列を含有するリクエスト

●RCE
exec、base64_decode、cmd= などを用いて サーバ上で任意コードの実行を狙う リクエスト

●SCAN
admin,wp-admin,.env等の一般に管理者ページのURL,環境情報を検索するリクエスト

●PROTO_POLLUTION
Javascriptの“__proto__” などのオブジェクトを上書きすることで、アプリケーションの挙動改変を狙う攻撃リクエスト(Next.js で多く観測)

●SQL_INJECTION
入力文字のサニタイジング漏れによるSQL文の挿入を狙った攻撃リクエスト

●XSS
script 等を埋め込み、ブラウザ上で不正なスクリプトを実行させることで、情報窃取や不正遷移を狙うリクエスト

●IOT_SDK_ENUM
IoT機器が使用している言語やAPI、環境を調べるためのリクエスト

●IOT_MALWARE
Iotを狙ってマルウェアを感染、実行させるためのリクエスト

●BOTNET_DOWNLOAD
サーバを Bot 化するため、外部からマルウェアをダウンロードおよび実行させることを狙うリクエスト

●LOG4SHELL
javaのログライブラリに含まれる脆弱性を狙った攻撃リクエスト

●APACHE_CGI_TRAVERSAL_RCE
ApacheのCGIに含まれる脆弱性を狙った攻撃リクエスト

●VMWARE_VCENTER_API
VMware vCenter Serverの脆弱性を狙った攻撃リクエスト

●NEXTJS_SERVER_ACTIONS_RCE
Next.js(13以降)のServer Actions 機能を悪用したリモートコード実行