平成 27 年 2 月 25 日

Topic

Bash の脆弱性[i]を標的としたアクセスの観測について（第 4 報）

Bash の脆弱性を標的とした宛先ポート 80/TCP に対するアクセスを多数観測しました。脆弱性の存在するウェブサーバがこのアクセスを受けると、不正な Perl スクリプトがダウンロードされ、ボットとして動作する可能性があります。ウェブサーバの脆弱性の有無の確認とセキュリティ対策を行うことを推奨いたします。

1 Bash の脆弱性を標的とした宛先ポート 80/TCP に対するアクセスの観測について

2 月 18 日から 2 月 24 日までの間、Bash の脆弱性を標的としていると考えられる宛先ポート 80/TCP に対するアクセスが増加しました。

Bash の脆弱性を標的とした宛先ポート 80/TCP に対するアクセスは、脆弱性の存在するウェブサーバの探索や、脆弱性の存在するウェブサーバへの侵入や攻撃を目的として送信されているものです。このアクセスは、以前から観測されており、これらの多くは細工したパケットを送信することにより、脆弱性の存在するウェブサーバ上で不正に Perl コマンドを実行させることを企図したものです。

今回増加したアクセスは、同様に Perl コマンドを実行させるものですが、Perl スクリプトを攻撃対象であるウェブサーバにダウンロード及び実行をさせ、当該ウェブサーバをボットとして利用することを目的としていると考えられます（図 1）。

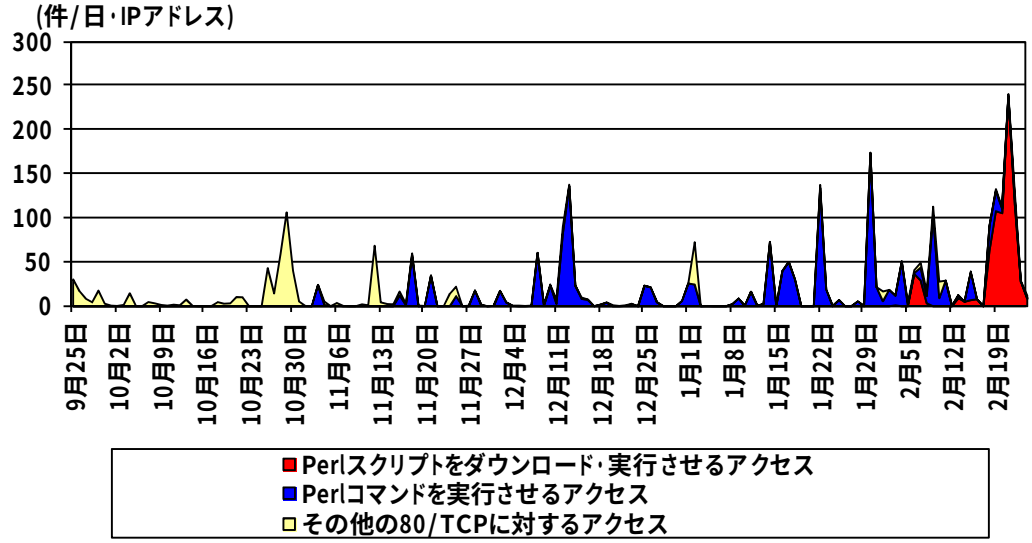

図 1 Bash の脆弱性を標的とした宛先ポート 80/TCP に対するアクセス件数の推移
（平成 26 年 9 月 25 日～平成 27 年 2 月 25 日）

---

i Bash の脆弱性に関しては、これまでにも複数回注意喚起を実施しています。
「Bash の脆弱性を標的としたアクセスの観測について」（平成 26 年 9 月 25 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140925-2.pdf
「Bash の脆弱性を標的としたアクセスの観測について（第 2 報）」（平成 26 年 10 月 7 日））
http://www.npa.go.jp/cyberpolice/detect/pdf/20141007.pdf
「Bash の脆弱性を標的としたアクセスの観測について（第 3 報）」（平成 26 年 12 月 9 日））
http://www.npa.go.jp/cyberpolice/detect/pdf/20141209-2.pdf

2　被害に遭ったウェブサーバの動作について

脆弱性の存在するウェブサーバがこのアクセスを受けた場合、ウェブサーバでは次のような動作が行われる可能性があります。

- Perl コマンドによる脆弱性有無の通知
- Perl スクリプトをダウンロード
- 当該 Perl スクリプトの実行（IRC ボットとしての動作）
  - 指令サーバへの接続
  - 各種不正動作
- 当該 Perl スクリプトの削除

この Perl スクリプトは、IRC ボットとして動作させるためのものであり、被害に遭ったウェブサーバは、外部に設置された指令サーバ（IRC サーバ）に対して宛先ポート 6667/TCP、チャンネル名「#bash」で接続を行います。そのサーバからの指令により、被害に遭ったウェブサーバは外部への DoS 攻撃、ポートスキャン、メール送信等の不正な動作をする危険性があります（図 2）。

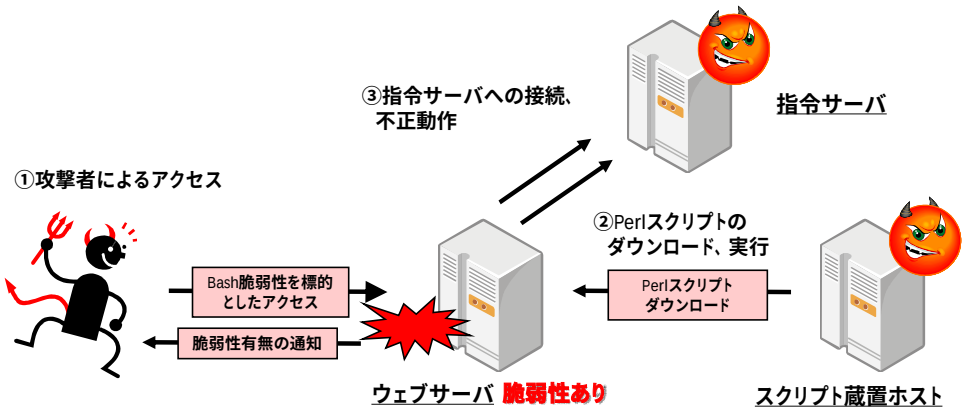

図2　被害に遭ったウェブサーバの動作

当該 Perl スクリプトは、実行後削除されますが、被害に遭ったウェブサーバのボットとしての動作は継続しているものと考えられます。また、攻撃者から更なる攻撃を受けている可能性があります。

3　推奨する対策

管理するウェブサーバが当該脆弱性の影響を受ける Bash を使用していないか確認してください。

脆弱性の公開から既に 5 ヶ月が経過し、様々な攻撃が行われてきたことを確認しています。脆弱性の存在を確認した場合は、今回紹介した事例以外にも外部から何らかの攻撃を受けている可能性が高いため、外部とのネットワーク接続を直ちに遮断し、詳細な調査を実施するとともにセキュリティ対策を行うことを推奨いたします。