平成 26 年 12 月 9 日

インターネット観測結果等

(平成 26 年 10 月期)

- **サーバ管理ソフトウェア Webmin を標的としたアクセスの急増**
- **宛先ポート 9064/TCP に対するアクセスの増加**
- **宛先ポート 0/TCP に対するアクセスの増加**

1　サーバ管理ソフトウェア Webmin を標的としたアクセスの急増

9月下旬に Bash の脆弱性が公表されて以降、宛先ポート 10000/TCP に対するアクセスの急増を観測しました（図1）。

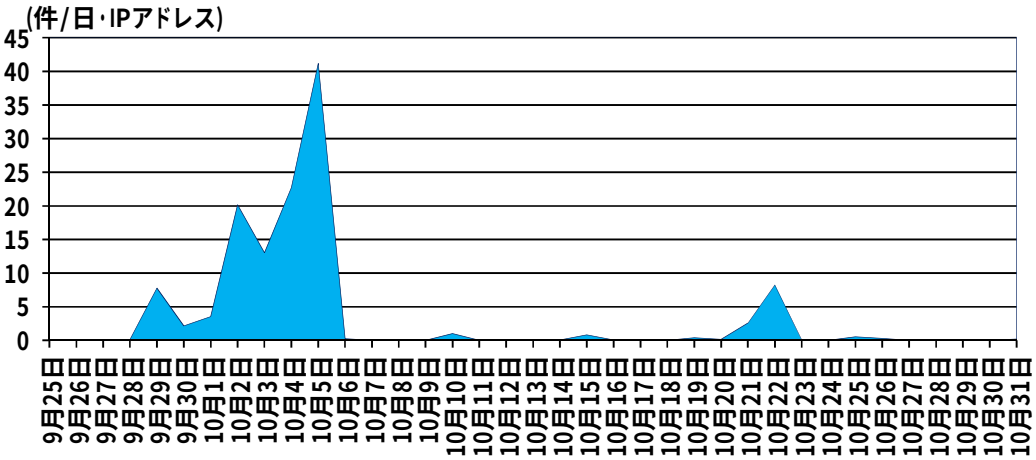

図1　宛先ポート 10000/TCP に対するアクセス件数の推移（H26.9.25～H26.10.31）

10000/TCP はサーバ管理ソフトウェア Webmin がデフォルトで使用するポートです。観測されたパケットの多くは、Webmin の CGI に対する接続要求であり、Webmin が稼動している機器を探索しているものと考えられます。

また、観測されたパケットの中には Bash の脆弱性に対する攻撃コードも存在したことから、攻撃者により Webmin が稼動していることを確認された場合には、Bash の脆弱性を利用した攻撃に遷移する可能性もあります。

警察庁では、10 月 7 日に Bash の脆弱性について注意喚起[i]を行っています。

[i] 「Bash の脆弱性を標的としたアクセス観測について（第 2 報）」（平成 26 年 10 月 7 日）
http://www.nap.go.jp/cyberpolice/detect/pdf/20141007.pdf

2　宛先ポート 9064/TCP に対するアクセスの増加

10 月上旬以降、宛先ポート 9064/TCP に対するアクセスの増加を観測しました（図2）。

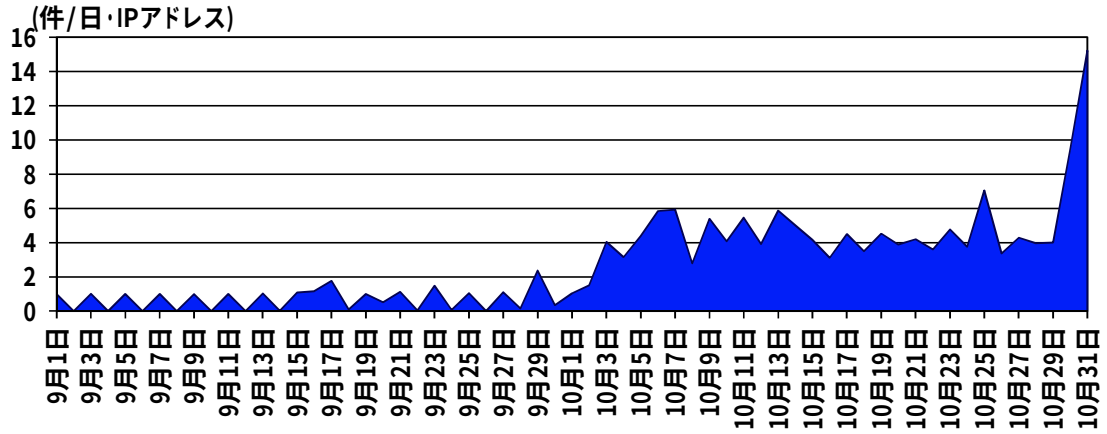

図2　宛先ポート 9064/TCP に対するアクセス件数の推移（H26.9.1～H26.10.31）

観測されたアクセスの内容を確認したところ、パケットの多くは HTTP の GET リクエストであり、プロキシサーバを探索するアクセスと考えられます。

3　宛先ポート 0/TCP に対するアクセスの増加

10 月 6 日、7 日及び 21 日に、宛先ポート 0/TCP に対するアクセスの増加を観測しました（図3）。

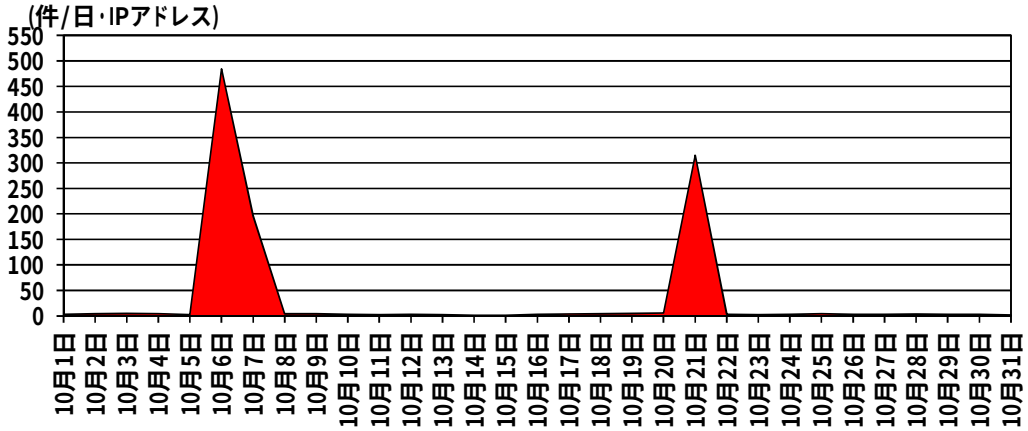

図3　宛先ポート 0/TCP に対するアクセス件数の推移（H26.10.1～H26.10.31）

宛先ポート 0/TCP は Reserved（予約済）ポートであり、ネットワークのサービスで使用すべきではないポートです。検知したパケットは、複数の国･地域を発信元としていますが、TTL の値が概ね一定であることから、発信元 IP アドレスを詐称している可能性も考えられます。

警察庁では、以前から同様のパケットを観測しており、目的は不明ですが、何者かが長期にわたってこれらのパケットを送っている可能性が考えられます。