平成 26 年 10 月 7 日

インターネット観測結果等

(平成 26 年8月期)

- サーバ管理チップの脆弱性を狙ったアクセスの急増
- 宛先ポート 53413/UDP に対するアクセスの急増
- JDWP(Java Debug Wire Protocol)に対する探索行為の検知

1 サーバ管理チップの脆弱性を狙ったアクセスの急増

8月 28 日以降、宛先ポート 49152/TCP に対するアクセスが急増しています（図1）。

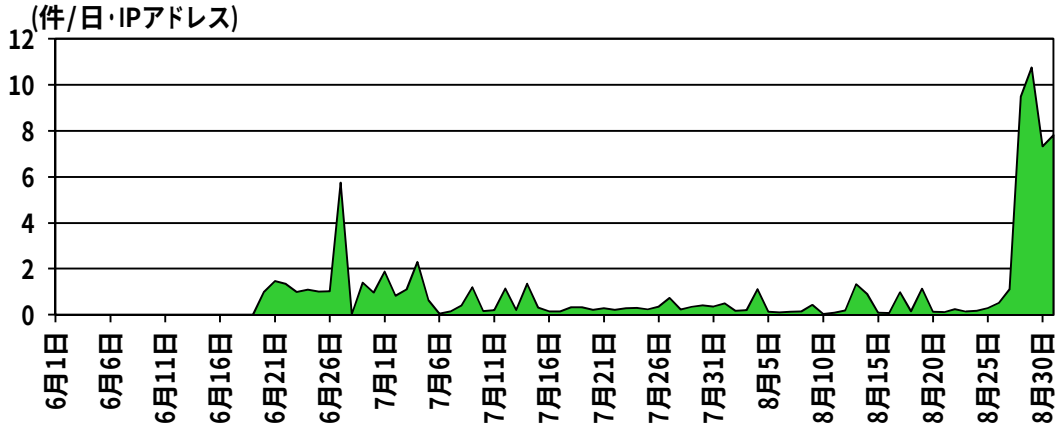

図1 宛先ポート 49152/TCP に対するアクセス件数の推移（H26.6.1～H26.8.31）

49152/TCP は、特定のメーカが製造するマザーボードに搭載された BMC[i]によって提供されるサーバ管理機能で使用されるポートであり、このポートに特定のリクエストを送信するだけで BMC 内に保存されたパスワードが閲覧可能となる脆弱性が存在します[ii]。そのため、このポートに対するアクセスは、脆弱性を持つ同製品に対する探索行為であると考えられます。

このポートに対するアクセスの発信元 IP アドレスについて調査を行ったところ、ルータや監視カメラのものと思われるログイン画面が散見されました。何者かが、これらの機器を踏み台にして、脆弱性を持つ機器やサービスを探索していることが推測されます。

インターネットに接続されたルータや監視カメラ等の機器において、推測されやすい ID やパスワードが設定されていたり、これらの機器の脆弱性が利用されたりした場合には、攻撃者は、インターネット上からこれらの機器にログインすることができます。

---

[i] Baseboard Management Controller。システムのハードウェア障害等を監視するためのチップ

[ii] インターネット観測結果等（平成 26 年 6 月期）
http://www.npa.co.jp/cyberpolice/detect/pdf/20140722.pdf

2　宛先ポート 53413/UDP に対するアクセスの急増

8月 27 日以降、宛先ポート 53413/UDP に対するアクセスの急増を観測しました（図2）。

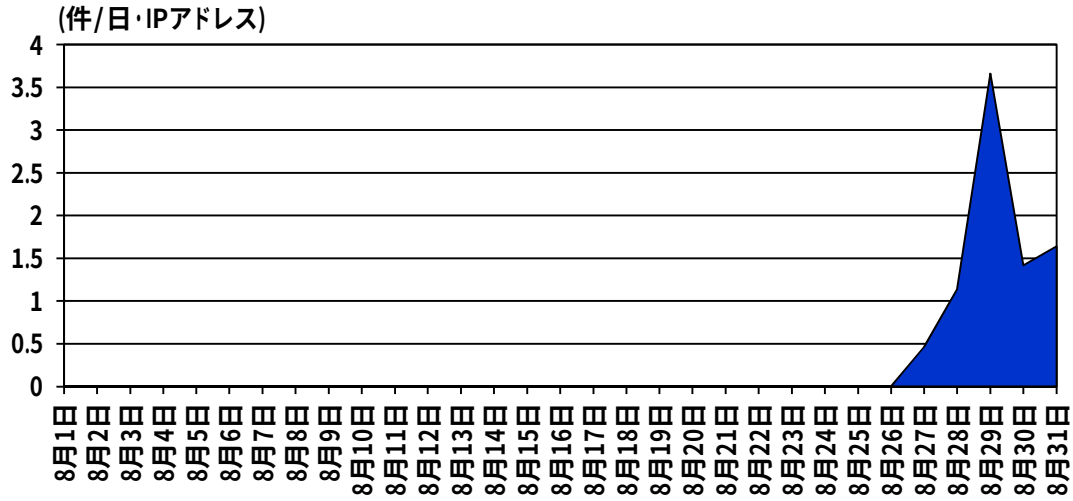

図2　宛先ポート 53413/UDP に対するアクセス件数の推移（H26.8.1～H26.8.31）

53413/UDP は、国外の特定のメーカが製造するルータで使用されているポートであり、8 月 27 日、攻撃者が外部から簡単にアクセスできる脆弱性が存在するとの情報がインターネット上に報告されています。

そのため、このポートに対するアクセスは、脆弱性を持つ同製品に対する探索行為である可能性が考えられます。

3　JDWP(Java Debug Wire Protocol)に対する探索行為の検知

6月 19 日以降、JDWP の探索行為と考えられるパケットを断続的に観測しました（図3）。

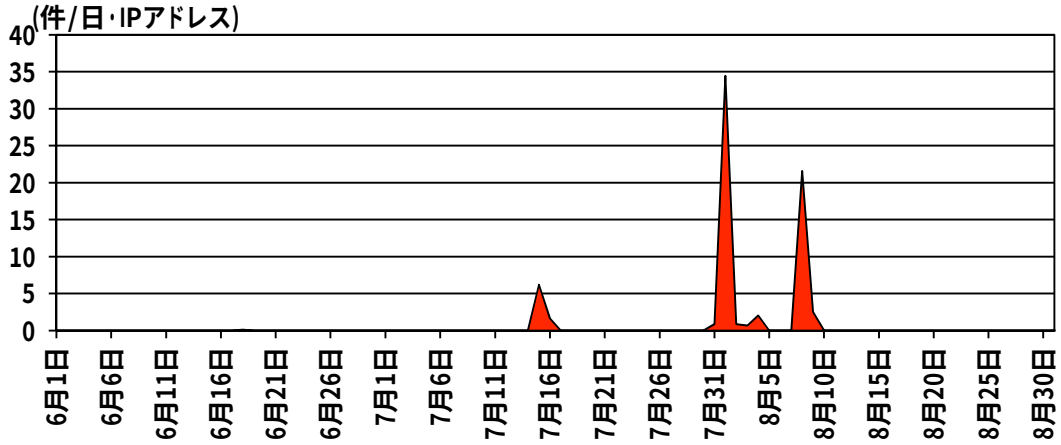

図3　JDWP の探索行為と考えられるパケット件数の推移[i]（H26.6.1～H26.8.31）

JDWP は Java アプリケーションをリモートでデバッグする際に使用されるプロトコルであり、次の手順で通信の確立を行います。

・デバッガから Java 仮想マシン（VM）に、文字列「JDWP-Handshake」が送信される。

・VMから、同じ文字列が返送される。

警察庁の定点観測システムでは文字列「JDWP-Handshake」を含むパケットを検知しており、当該パケットは JDWP の探索行為であると考えられます。また、同プロトコルを使用するポートは任意に設定することができるため、複数のポートでパケットを検知しています[ii]。

適切な対策を施さずに Java アプリケーションをインターネット上からリモートでデバッグする機能を有効にしている場合、攻撃者に侵入され、任意の Java コードを実行される恐れがあります。

警察庁では、9月5日に注意喚起[iii]を実施していますので、対策等については、そちらを確認し下さい。

---

[i] 6月 19 日のパケット件数はごく僅かであるため、グラフ上には表示されていない。

[ii] 警察庁の定点観測システムでは、ポート 1044、4000、5005、8000、8001、8011、8080、8787、8788、8822、8888、8889、9009、9999/TCP で同パケットを検知した。

[iii] 「JDWP(Java Debug Wire Protocol)に対する探索行為の検知について」（平成 26 年9月5日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140905.pdf