平成 27 年 12 月 15 日

Topic

IoT 機器を標的とした攻撃の観測について

インターネットに接続されたデジタルビデオレコーダ等の Linux が組み込まれた IoT 機器を標的とした攻撃を観測しています。この攻撃を受けた機器が、攻撃者の命令に基づいて動作する「ボット」になる事例を確認しています。現在利用している機器について、最新のセキュリティ情報を確認することを推奨いたします。

1 宛先ポート 23/TCP に対するアクセス

23/TCP はネットワークに接続された機器を遠隔で操作する Telnet で利用されていますが、このポートに対するアクセスは、平成 26 年以降、高い水準で推移しています。

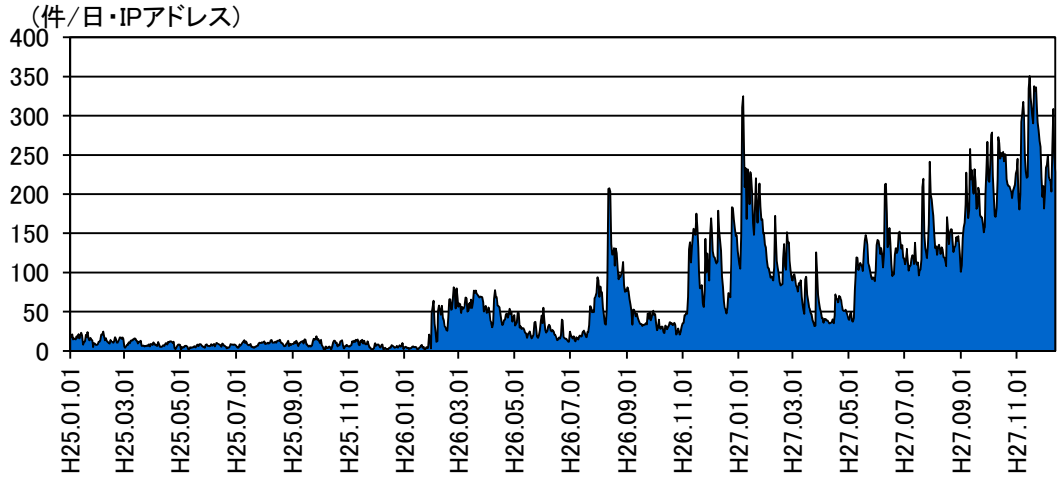

図1 宛先ポート 23/TCP に対するアクセス件数の推移

これらのアクセスについては、過去にも注意喚起を実施してきたように、多くはインターネットに接続されたルータ、ウェブカメラ、ネットワークストレージ、デジタルビデオレコーダ等の Linux が組み込まれた IoT 機器（以下「組み込み機器」という。）が発信元であることを確認しています[i]。これらの機器は、何らかの手法により、攻撃者に乗っ取られ、攻撃の踏み台として悪用されていると考えられます。

[i] 「インターネット観測結果等(平成 26 年 11 月期)」（平成 26 年 12 月 18 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141218.pdf
「インターネット観測結果等(平成 27 年9月期)」（平成 27 年 10 月 28 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17084

2　組み込み機器を標的とした攻撃

宛先ポート 23/TCP に対するアクセスについて分析を行ったところ、不正なプログラムをダウンロードして実行させる攻撃が存在していることを確認しました。この不正なプログラムは、特定の CPU で動作する Linux に感染するものであり、一般のコンピュータで広く採用されている CPU「X86」で動作する Linux には感染しないものでした。CPU「ARM」「MIPS」「PowerPC」「SuperH」を標的とした不正なプログラムであることを確認しています。

これらの CPU は、組み込み機器で多く利用されているものであり、攻撃者は、インターネットに接続された組み込み機器を標的として攻撃を行っていると考えられます。

この不正プログラムに感染すると、Telnet や HTTP により C&C（Command and Control）サーバに接続を行い、攻撃者からの命令に基づいて動作する「ボット」になってしまいます。感染した機器の挙動として、感染拡大を狙ったさらなる探索（Telnet 探索、宛先ポート 53413/UDP に対するアクセス）等を確認しています（図2）。ボット化した機器は、攻撃者の設定する命令による感染拡大の他、DDoS 攻撃やスパムメールの送信等に悪用される可能性があります。

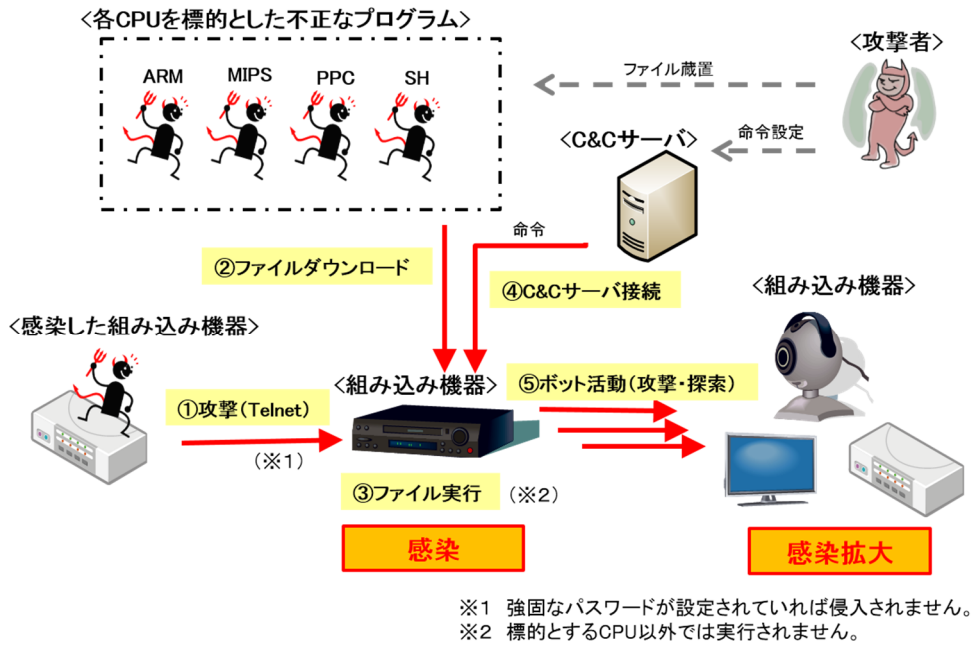

図2　組み込み機器を標的とした攻撃と感染の拡大

今回確認した宛先ポート 53413/UDP に対するアクセスは、国外の特定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、当該ルータの探索と考えられます。このルータについては、脆弱性が報告されており、攻撃者は脆弱性を突いて、ボットの感染拡大を企図していると考えられます。11 月下旬頃から、アクセス件数が増加していることを確認しています（図3）。

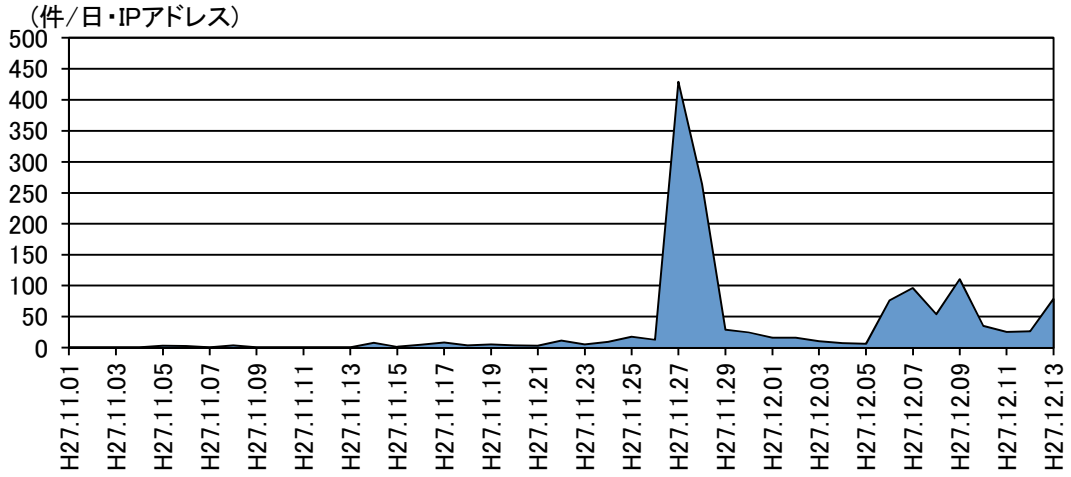

図3　宛先ポート 53413/UDP に対するアクセスの推移

なお、IoT 機器を標的とした攻撃については、横浜国立大学、国立研究開発法人情報通信研究機構（NICT）及びドイツザールラント大学による研究成果（IoTPOT: Analysing the Rise of IoT Compromises）が報告されています[i]。

3　推奨する対策

今後、IoT のさらなる普及に伴い、様々な機器がインターネットへの接続機能を持つようになり、IoT 機器が攻撃の標的となることが懸念されます。IoT 機器は、処理能力の低下等、機器の異常に利用者が気付くことが難しいものも多く、そのため、不正なプログラムへの感染や攻撃を受けている状況を把握することが困難となることがあります。

現在利用している機器について、最新のセキュリティ情報を確認してください。また、メーカサポートが終了した製品を使用し続けることは、脆弱性に対するソフトウェア等の修正が行われない可能性があるため非常に危険です。

IoT 機器の利用者は、予期せぬ被害に遭わないために IoT 機器への脅威が増加している状況を把握し、セキュリティ意識を高く持ってこれらの機器を利用していく必要があります。

[i] 「IoTPOT:Analyzing the Rise of IoT Compromises」
https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf
https://www.usenix.org/sites/default/files/conference/protected-files/woot15_slides_papa.pdf