平成 28 年9月 30 日

インターネット観測結果等

（平成 28 年8月期）

- FreePBX の脆弱性を標的としたアクセスを観測
- SSDP に使用される宛先ポート 1900/UDP に対するアクセスが増加
- 宛先ポート 23/TCP に対するアクセスの発信元 IP アドレス数が急増

1　FreePBX の脆弱性を標的としたアクセスを観測

FreePBX は、IP 電話交換機用のソフトウェアである Asterisk の設定・管理用ツールです。

平成 28 年8月９日に、FreePBX で使用される特定のモジュールに存在する深刻な脆弱性が開発元から公表[i]されました。当該脆弱性を悪用し、特別に細工したリクエストを送信することによって、任意のコマンドを実行できるとされています。また、8月 12 日には、当該脆弱性に対する探索等を行うツールがインターネット上で公開されていることも確認しています。

警察庁のインターネット定点観測システムにおいては、8月 16 日から探索ツールの特徴を有したアクセスを観測しました。これらのアクセスは、FreePBX の特定のファイルを標的とした HTTP リクエストでした（図1）。

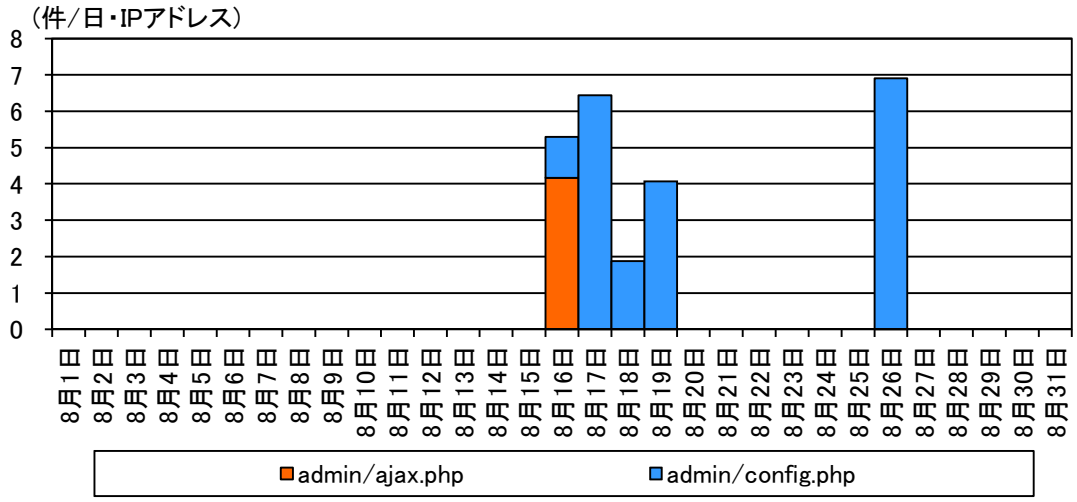

図1　FreePBX の特定のファイルを標的としたアクセス（リクエストファイル別）

アクセスの内容を分析したところ、admin/config.php に対して FreePBX のバージョン情報の取得を試みるアクセス及び admin/ajax.php に対して脆弱性の有無を確認するアクセスが確認できました。

[i] 2016-08-09 CVE Remote Command Execution with Privileged Escalation - FreePBX OpenSource Project - Documentation
http://wiki.freepbx.org/display/FOP/2016-08-09+CVE+Remote+Command+Execution+with+Privileged+Escalation

当該脆弱性を悪用されると不正にコマンドが実行され、結果として深刻な被害を受ける危険性があります。当該脆弱性の影響を受けるバージョンの FreePBX を利用している場合は、脆弱性が修正されたバージョンへの速やかなアップデートを推奨します。開発元によると、影響を受ける FreePBX とモジュールである System Recordings Module のバージョンの組合せは以下のとおりです。

- FreePBX 13 及び FreePBX 14
- System Recordings Module 13.0.1beta1 から 13.0.26

2 SSDP に使用される宛先ポート 1900/UDP に対するアクセスが増加

SSDP（Simple Service Discovery Protocol）は、ネットワーク機器同士の接続機能である UPnP（Universal Plug and Play）で使用されるプロトコルです。警察庁のインターネット定点観測システムでは、平成 26 年9月上旬頃に SSDP で使用されるポート 1900/UDP に対するアクセスの増加を観測[i] して以降、継続的に同アクセスを観測していましたが、今期の8月中旬頃に同ポートに対するアクセスが増加しました（図2）。

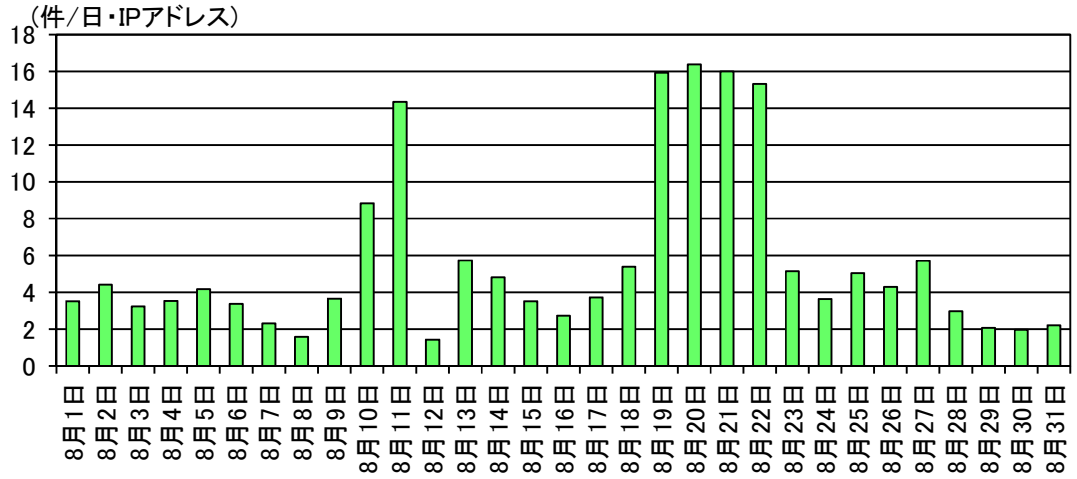

図2 宛先ポート 1900/UDP に対するアクセス件数の推移

観測したアクセスは、機器情報の送信を要求する「M-SEARCH」メッセージがほとんどで、このメッセージに応答するネットワーク機器の探索行為が行われていると考えられます。外部からの「M-SEARCH」メッセージに応答するネットワーク機器が攻撃者に発見された場合、SSDP リフレクター攻撃（図3）の踏み台として悪用される危険性があります。

[i] 「UPnP に対応したネットワーク機器を踏み台とした SSDP リフレクター攻撃に対する注意喚起について」（平成 26 年 10 月 17日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf

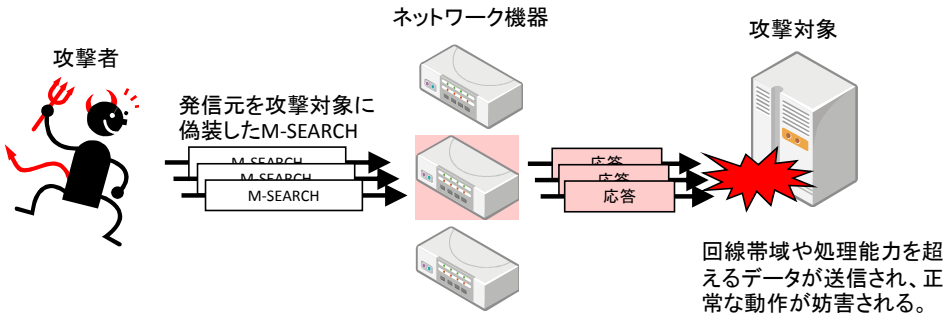

図3　SSDP リフレクター攻撃の概要

管理するネットワーク機器が SSDP リフレクター攻撃の踏み台として悪用されないために、次の対策を実施することを推奨します。

- 外部からの SSDP プロトコル通信（宛先ポート 1900/UDP のパケット）を遮断する。
- ネットワーク機器の UPnP 機能を使用していない場合は、停止する。
- ネットワーク機器の UPnP 機能を使用する場合は、外部からの「M-SERACH」メッセージに対して応答しないように設定する。

3　宛先ポート 23/TCP に対するアクセスの発信元 IP アドレス数が急増

今期は、宛先ポート 23/TCP に対するアクセスの発信元 IP アドレス数が急増し、国内の発信元 IP アドレスも併せて増加しました（図4）。

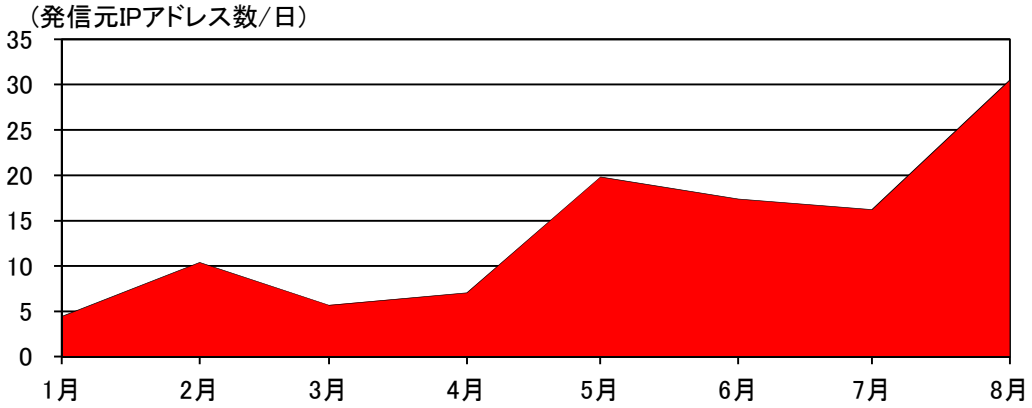

図4　宛先ポート 23/TCP に対するアクセスの発信元 IP アドレス数の推移
（日本国内、平成 28 年 1 月～8月、一日当たりの平均値）

23/TCP は Telnet で使用されるポートです。そのため、これらのアクセスは Telnet でログイン可能なコンピュータやネットワーク機器の探索を目的としているものと考えられます。また、これらのアクセスを分析したところ、センサー到達時の TTL 値が 64 未満のものが 99.3%を占めていました（図5）。

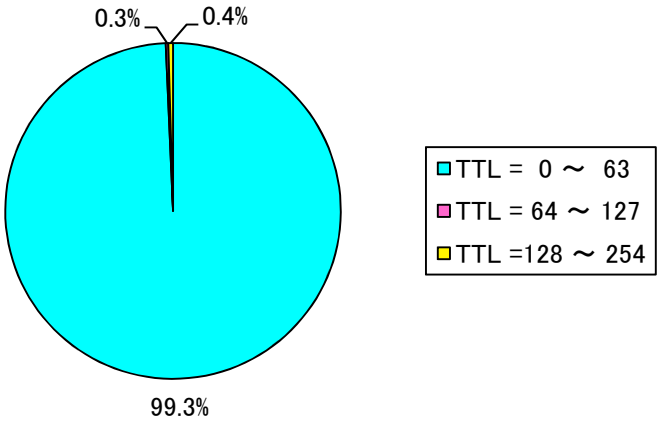

図5　宛先ポート 23/TCP に対するアクセスにおける TTL 値別比率（平成 28 年8月）

TTL 値は OS により初期値が異なり、Linux 系 OS や MacOS の場合は 64、Windows の場合は 128、Solaris や Unix の場合は 255 となっています。そのため、当該アクセスの発信元は Linux 系 OS の機器である可能性が高いと考えられます。

国内における当該アクセスの発信元を調査したところ、デジタルビデオレコーダー、ウェブカメラ、ルータ等の特徴が見られるものが多くありました。そのため、これらの IoT 機器が攻撃者に乗っ取られ、攻撃者の命令に基づいて動作するボットとして動作し、ボットの感染拡大を目的として Telnet 探索を行っている可能性があります。また、発信元 IP アドレス数が増加していることから、以前よりもボットの感染が拡大している可能性が高いと考えられます。