2017 年 12 月号

SQAT® 情報セキュリティ瓦版

IoT の新たな脅威 “Reaper”

「IoT の脅威」というと、昨年猛威を振るった「Mirai」が知られています。その被害が未だ記憶に新しい中、Mirai から進化した新たな脅威「Reaper」が、本年 10 月に発見・報告されました。

なお、Reaper が登場するまでの間には、「Hajime」というボットネットも発見・報告されています（2017 年 4 月）。この Hajime と比較すると、今回の Reaper は、暗号化や機能などの面では劣るものの、感染台数の規模の大きさは圧倒的であり、今後巨大なボットネットが形成される可能性が懸念されます。

また、将来的には、Reaper のような拡散力と Hajime のような高機能性の両方を備えたボットネットが登場することも予想されます。ボットネットの進化の先を読み、対策面・運用面での対応に着手する必要性は、これまでになく高まっていると言えるでしょう。

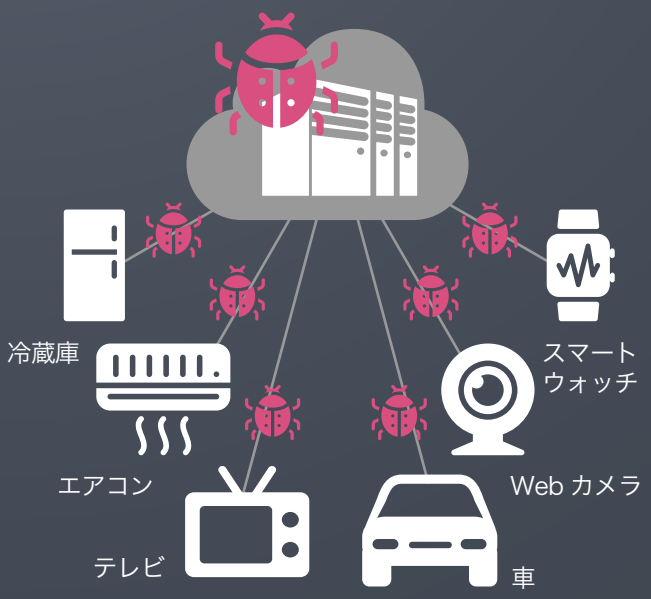
では、サイバー攻撃を受け、自組織のシステムがボットネットの一端となってしまった場合、どのような事態が発生するのでしょうか。

被害報告によると、「通信先である C&C サーバから指令を受けて外部への DDoS 攻撃を行った」、「迷惑メールの送信の中継に使われた」等の事態に至り、結果として、犯罪に意図せず加担してしまったというケースが多数報告されています。そのほかのシナリオとしては、安全制御装置をはじめとする各種機能が改変されてしまう等の深刻な事態も想定されます。

IoT とは、身近にある「モノ」が通信機能を持つことであり、IoT の脅威はどこにでもありえる、ごく身近な脅威です。その反面、これから社会に根付こうとする黎明期のテクノロジーに対するリスクの認識は、まだまだ乏しいのが現状です。

しかし、脅威は既に内包されています。攻撃側も、IoT というテクノロジーの進化と同じ速さで進化している、という認識のもと、対応していくべきでしょう。

対策として、単一ソリューションのみに頼るのではなく、エンドポイント対策やネットワーク監視など、複数のソリューションを組み合わせることを推奨いたします。



IPA - JVN iPedia
2017 年第 3 四半期活動報告レポートを発行

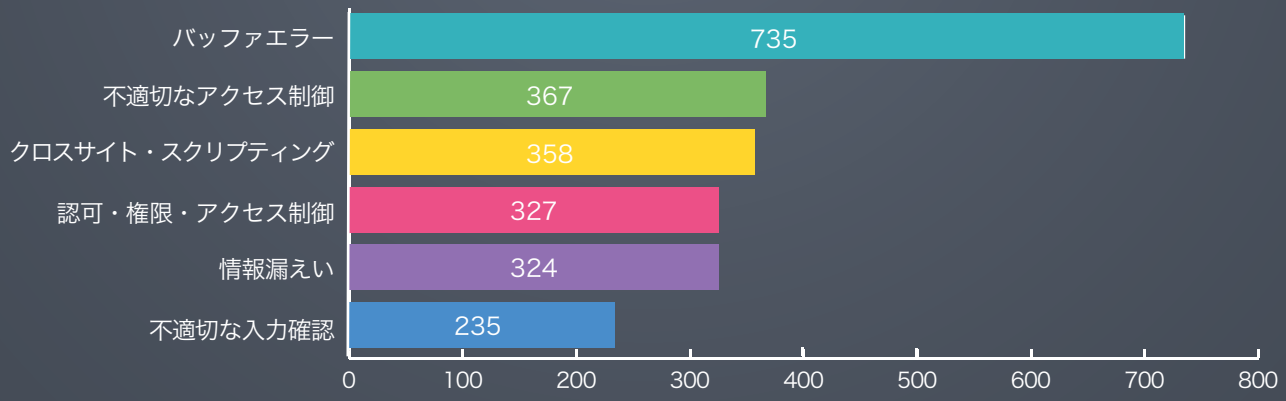
2017 年 10 月 24 日、IPA は、『脆弱性対策情報データベース JVN iPedia に関する活動報告レポート』2017 年第 3 四半期版を発行しました。その中から、要注目情報をご紹介します。

最初に取り上げたいのは、Bluetooth の脆弱性である「BlueBorne」と、Apache Struts2 です。両者に共通するのは、「深刻度の高い脆弱性が複数登録されている」、「悪用された場合の影響が大きい」、「IPA から緊急対策情報等が発信されている」という指摘です。さらに、Apache Struts2 については実際に大規模な情報漏洩事件が発生しています。こうした事態を鑑み、同レポートでは、早急に対策を講じる必要があることを改めて呼びかけています。

脆弱性の種類別件数に関しては、「バッファエラー（CWE-119）」が 735 件と、2 位以下を大きく引き離して最も多く登録されています（下図参照）。バッファに関するエラーは、主要なソフトウェアにおいても多数報告されており、深刻な影響につながる可能性があります（下表参照）。

組織で使用されている IT 資産の脆弱性情報に常に注意を払うとともに、アップグレードや最新パッチの適用を徹底するといった基本的な対策を怠らないことが肝要と言えるでしょう。

脆弱性の種類別件数



出典：IPA：脆弱性対策情報データベース JVN iPedia に関する活動報告レポート
［2017 年第 3 四半期（7 月～ 9 月）］

バッファに関するエラーの例：バッファオーバーフロー（別名：バッファオーバーラン）の攻撃例

攻撃者による任意コードの実行	ウィルスの混入／ファイル削除／情報漏えい（機密性、または完全性に関する問題）
システム破壊	システム停止（可用性に関する問題）
想定外動作	誤作動（可用性に関する問題）

修正パッチの公表以降に被害が多発 ～速やかな対処を求められるセキュリティ対策

2017 年 9 ～ 10 月にかけて、Apache Tomcat の重大な脆弱性が次々と明らかになり、世間を大いに騒がせました（下図参照）。

一連の脆弱性は、リモートから攻撃者が任意のコードを実行でき、情報漏えいの可能性を生むことから、大変危険な状態であると認識されました。

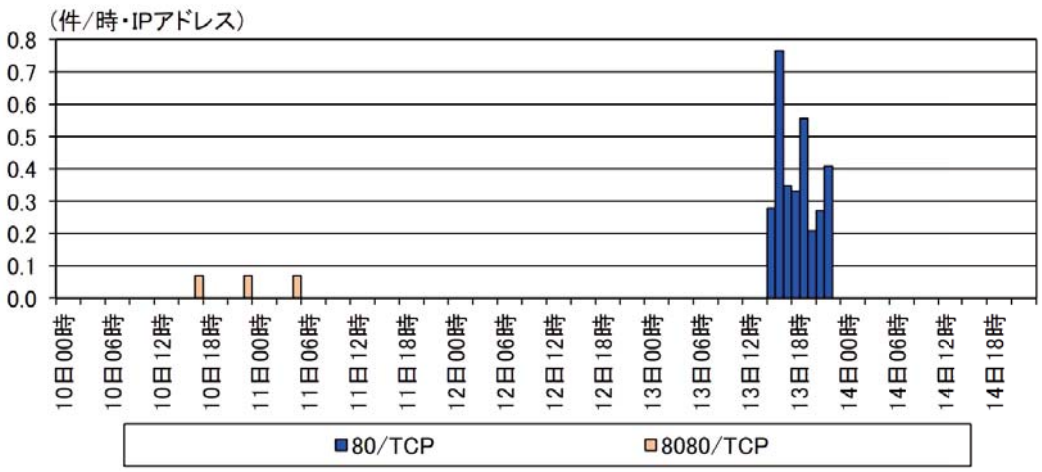
これらの脆弱性は、JPCERT/CC による注意喚起を通じて広く知られることになった一方で、ベンダーからのパッチ提供には時間を要しました。この点も、世間の注目を集めることになった一因と言えます。

実のところ、現在、いわゆる「ゼロデイ攻撃」を実行できるほど高度なテクニックをもつ攻撃者は、それほど多くは存在しません。
時間の経過や、PoC（発見された脆弱性を悪用した攻撃が実際に可能であることを実証しているコード）が出回ることなどにより、攻撃の難易度が下がるような条件が揃うと、他の大多数の攻撃者も攻撃可能な状態となるのです。

Apache Tomcat における脆弱性に関する注意喚起

脆弱性（CVE-ID）	影響を受ける Apache Tomcat のバージョン
CVE-2017-12615	7.0.0 ～ 7.0.79
CVE-2017-12616	7.0.0 ～ 7.0.80
CVE-2017-12617	9.0.0.M1 ～ 9.0.0 8.5.0 ～ 8.5.22 8.0.0.RC1 ～ 8.0.46 7.0.0 ～ 7.0.81

Apache Tomcat の脆弱性（CVE-2017-12617）を標的としたアクセスの宛先ポート別件数の推移



出典：警視庁：Apache Tomcat の脆弱性（CVE-2017-12617）を標的としたアクセスの観測について

そのため、ゼロデイ攻撃よりも、むしろ、修正パッチが公開されてから実際に適用されるまでの期間のほうが、セキュリティ的には危険な状態であると考えられます（警視庁が公表した資料にも、当該脆弱性に関連する HTTP リクエストを観測したのは、パッチ公表以降である旨が記載されています）。

こうした傾向は、2017 年 5 月に流行したランサムウェア「WannaCry」や近年頻発している Apache Struts2 関連の事案でも同様であり、修正パッチが公表されて以降の被害が目立つ状況となっています。

攻撃を未然に防ぐには、組織内で使用している IT 資産に関する脆弱性情報を収集し、それに応じた対策を講じることが必要です。

もっとも、脆弱性に関する情報は膨大で、かつ、日々更新されるため、リアルタイムのキャッチアップには相応の労力がかかります。情報の収集、分析、意思決定を効率的に遂行する上で、必要に応じて社外のセキュリティ専門家を活用することをお勧めします。

一口メモ

Apache Tomcat は、Java を使った動的な Web ページを動作させます。それと同時に Web サーバとしての機能も利用可能です。
ちなみに、似たような名前と機能で混同されることが多い「Apache」（または「Apache HTTP Server」）は、Web サーバとしての機能がメインの別プロダクトです。Java 環境では Web サーバとして Apache、Java の動作用として Apache Tomcat を採用する組織が多い傾向となっています。

株式会社ブロードバンドセキュリティ
本　社　〒160-0023　東京都新宿区西新宿 8-5-1　野村不動産西新宿共同ビル 4F
TEL：03-5338-7417　FAX：03-5338-7435　https://www.bbsec.co.jp/