YNU 横浜国立大学 YOKOHAMA National University

Press Release
2021 年 6 月 9 日

〒240-8501 横浜市保土ケ谷区常盤台 79-1

IoT サイバー攻撃の大規模観測データの提供開始

独自の観測システムで収集したサイバーセキュリティインテリジェンスを無償提供

・モノのインターネット(Internet of Things: IoT)を構成する様々な機器がサイバー攻撃の対象となり、マルウェア感染する事例が増えています。感染機器からの攻撃を観測する独自の囮システム(ハニーポット)により収集された 17 万を超えるマルウェア検体、280 万を超えるマルウェアダウンロード URL を無償提供します。また、最新のサイバー攻撃の概況を Web サイトで公開いたします。
・加えて、独自のハニーポットにより観測される反射型分散サービス妨害攻撃の最新の状況を Web サイトで公開いたします。
・上記のサイバーセキュリティインテリジェンスは、研究開発・運用等にご活用頂けます。

【概要】
横浜国立大学大学院環境情報研究院／先端科学高等研究院の吉岡准教授らの研究グループは、マルウェア感染した IoT 機器からのサイバー攻撃を観測する囮システム(ハニーポット)や反射型分散サービス妨害攻撃(Distributed Reflection Denial of Service Attack: DRDoS Attack)をリアルタイムで観測するシステムを構築し、観測、分析を行ってきました。これまで世界 30 か国・地域以上の 100 を超える研究組織に観測結果を提供しています。
今回、サイバーセキュリティの研究開発の進展に資することを目的とし、これまでの提供内容を大幅に増強した観測データ(17 万を超えるマルウェア検体と 280 万を超えるマルウェアダウンロード URL)を研究開発者、実務者向けに提供することといたしました。
https://sec.ynu.codes/

【データセット概要】
今回提供するデータセットは、IoT 機器をターゲットとしたサイバー攻撃を観測し、マルウェアを収集する囮観測システムである IoT ハニーポット（IoTPOT）および反射型分散サービス妨害攻撃(Distributed Reflection Denial of Service Attack: DRDoS Attack)を観測するハニーポット（Amppot）により観測、収集されたデータに基づくものです。

IoT ハニーポット（IoTPOT）

IoT 機器への攻撃を観測する IoT ハニーポット（IoTPOT）を 2015 年から稼働させています。観測した攻撃数、収集した IoT マルウェア数、マルウェアのダウンロード URL 数などの統計データを Web ページ上で一般公開しました。また、収集した IoT マルウェア検体のデータセット、マルウェアのダウンロード URL のデータセットを研究者向けに提供します。

DRDoS ハニーポット（Amppot）

DRDoS とは、大量の通信によりサービスを妨害する攻撃の一種であり、インターネット上の複数のサーバに通信を反射させて通信量を増大させ、攻撃対象に送信する攻撃手法です。DRDoS 攻撃を観測するハニーポット（Amppot）を 2012 年から稼働させています。
観測した攻撃数、攻撃対象となっているポート番号などの統計データを Web ページ上で一般公開しました。また、観測された通信データを研究者向けに一部提供します。

【社会的な背景】

サイバー攻撃が世界各国で発生し国際的な問題となっています。加えて DX（デジタルトランスフォーメーション）やネットワーク技術の進展といった近年の動向を受け、「あらゆるデバイスがネットワークにつながる」と表現されることもあるように、膨大な数の機器がネットワークに接続され、機器の種類も多様になっています。このような状況により、サイバー攻撃は、生活や経済活動など広範囲で甚大な影響を及ぼす恐れがあります。そのため、多様化、高度化するサイバー攻撃の観測・分析・対策を行う実用性の高いサイバーセキュリティ技術が求められています。

【今後の展開】

実際に起こっているサイバー攻撃の観測・分析データはサイバーセキュリティの研究や技術開発にとって有益であり、Web サイト公開とデータセットの提供は、これらの研究開発を推進することが期待されます。
研究者向けのデータセット提供に加えて、今後、一般的の注意を促すような情報発信を工夫し、サイバー攻撃の事実を知ること、利用者が意図せずサイバー攻撃に加担する状況の発生を抑制するなど、サイバーセキュリティへの理解向上にも寄与して参ります。

【用語解説】

DRDoS (Distributed Reflection Denial of Service Attack: DRDoS Attack)：大量の通信によりサービスを妨害する攻撃の一種であり、インターネット上の複数のサーバに通信を反射させて通信量を増大させ、攻撃対象に送信する攻撃手法です。

【外部資金に関する情報】

国立研究開発法人情報通信研究機構(NICT)委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive)」、総務省委託研究「国際連携によるサイバー攻撃の予知技術の研究開発（PRACTICE)」、「電波資源拡大のための研究開発（JPJ000254)」における委託研究「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発」の成果を含みます。

本件に関するお問い合わせ先

横浜国立大学　大学院環境情報研究院/先端科学高等研究院　准教授　吉岡克成

TEL:045-339-4134 / メールアドレス：yoshioka@ynu.ac.jp