報道関係者各位
（参考資料）

2025 年 3 月 28 日
株式会社インターネットイニシアティブ

IIJ、DDoS攻撃に悪用されるマルウェア「Mirai」の解析ツールを開発し サイバーセキュリティ対策を行う事業者、アナリストに向け無償公開

-- IIJのセキュリティ事業やサイバー攻撃研究により社内に蓄積された知見を、コミュニティに還元 --

当社は、近年多発している大規模なサイバー攻撃（DDoS 攻撃）に悪用されるマルウェア「Mirai」とその亜種（以下、Mirai 等）の情報を分析するツール「mirai-toushi（ミライ トウシ）」を開発し、自社セキュリティサービスの運用等で活用するほか、セキュリティ事業者やセキュリティアナリスト向けに無償で公開いたします。mirai-toushi は、Mirai 等のプログラム内部に共通して記録される情報を自動的に抽出する機能があり、本ツールを利用することで、Mirai 等に対して迅速な調査・解析が可能となり、攻撃の防止や感染拡大の抑止といった対策を早期に実施することが可能になります。

背景

近年発生している大規模なサイバー攻撃は、主にインターネットに接続された監視カメラや家庭用 Wi-Fi ルータなどがマルウェア（不正ソフトウェア）に感染し、攻撃者が感染した端末を悪用することで引き起こされています。使用されるマルウェアとしては、「Mirai」と、そのソースコードをもとに開発された多数の亜種が、特に多く観測されています（※1）。
感染による被害や感染拡大を防ぐためには、原則的にマルウェア 1 種類ごとにどのような挙動を行うのかを分析し対策する必要がありますが、Mirai には多数の亜種が存在するため、亜種それぞれに解析を行なうことは多大な労力と時間を要します。そこで当社は、数多くある Mirai 亜種の解析を自動で行えるツールを開発いたしました。このツールにより、解析作業の効率が大幅に向上し、攻撃の防止や感染拡大の抑止のための迅速な対応やセキュリティ対策の見直しなどが可能となります。
※1 Mirai は 2016 年にソースコードが公開されて以来、様々な攻撃者が独自に改造したり設定変更を加えたりし、現在もサイバー攻撃に悪用されている

mirai-toushi 概要

今回当社が開発した「mirai-toushi」は、Mirai 等の「検体」（※2）を分析するためのソフトウェアで、Mirai 等に共通してプログラム内部に暗号化されて記録されている情報を自動で抽出します。これにより、セキュリティアナリストは、短時間で非常に効率的に当該検体の解析を行うことが可能となります。
※2 検体：分析のために採取したマルウェアのプログラム等

mirai-toushi の主な特徴、活用例は以下のとおりです。

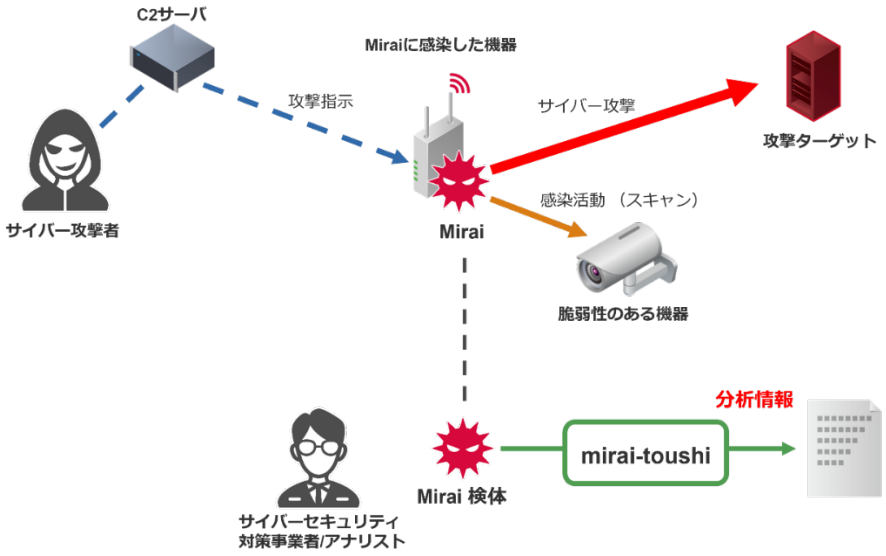
- C2 サーバ（※3）の情報を抽出し、感染機器への遠隔操作を無効化
  Mirai 等に感染した機器は、攻撃者からの指示のもとに、ターゲットへのサイバー攻撃を行ないます。mirai-toushi は、攻撃指示に利用される C2 サーバの情報を抽出できるため、その情報をもとにファイアウォールなどの設定を変更し通信を阻害することで、感染機器の動作を封じ込めてサイバー攻撃を停止させることが可能です。
  ※3 C2（Command and Control）サーバ：攻撃者の指示を感染機器に伝えるためのサーバ

- スキャン情報の抽出により、攻撃対象になりうる機器を把握可能
  Mirai 等は、インターネット上にあるデバイスをスキャンし、乗っ取り可能なデバイスに感染する機能を持っています。
  mirai-toushi を使用して Mirai 等からスキャンに利用される情報を抽出することで、その Mirai 等が

どういった機器を感染対象としているかを確認できます。また、多数の検体を分析することで、ターゲットにされやすい機器のトレンドを分析することができ、予防活動にも役立てることができます。

- 攻撃パラメータ情報の抽出により防御策の検討が可能
  Mirai 等は、攻撃者からの指示を受けてターゲットに対して DDoS 攻撃などのサイバー攻撃を実行します。mirai-toushi により攻撃に利用されるパラメータを抽出することで、ターゲットとなっているサーバがどのような防御策をとるべきかを検討することが可能になります。

■Mirai の挙動と mirai-toushi による検体解析のイメージ



mirai-toushi 公開 URL
https://github.com/iij/mirai-toushi

当社は、インターネットという重要な社会インフラをサイバーセキュリティの脅威から守るセキュリティビジネスを展開するとともに研究活動を推進しています。長年ビジネスで培ったセキュリティに関するノウハウを活かし、自社のインターネットバックボーンやセキュリティサービスから得られる膨大なログやイベント情報を情報分析基盤に集約して、セキュリティオペレーションセンター（SOC）での最新の脅威に対応するための研究活動にも活用しています。また当社はサイバーセキュリティコミニティの一員として、産官学のサイバーセキュリティ研究コミュニティとの連携を行なっており、今回提供を行なう mirai-toushi も、こうしたコミュニティへの貢献の一環として無償提供を行なうものです。
今後もさらに、国内外における関係団体およびコミュニティ活動を推進し、業界に当社の技術・知見を還元することで、安心・安全なインターネット社会の構築に貢献してまいります。

（参考情報）
開発者による本ツールの機能説明、実行方法などを IIJ エンジニアブログに掲載しています。
➢ IIJ エンジニアブログ： https://eng-blog.iij.ad.jp/archives/29246

また、mirai-toushi については、2025 年 5 月にフランスで開催されるセキュリティカンファレンス「Botconf 2025」に採択され、開発メンバが発表を行います。
発表日： 2025 年 5 月 21 日（水）16:00～16:40
タイトル： mirai-toushi: Cross-Architecture Mirai Configuration Extractor Utilizing Standalone Ghidra Script
URL： https://www.botconf.eu/botconf-2025/

報道関係お問い合わせ先
株式会社インターネットイニシアティブ　広報部　増田、荒井
TEL：03-5205-6310　FAX：03-5205-6377
E-mail：press@iij.ad.jp　URL：https://www.iij.ad.jp/