Distributed via @police
https://www.npa.go.jp/cyberpolice/

令和２年２月 26 日

レポート

宛先ポート 4567/TCP に対する Mirai ボットの特徴を有するアクセスの増加等について

- 宛先ポート 4567/TCP に対する Mirai ボットの特徴を有するアクセスの増加
- PJL(Printer Job Language)に対応した機器を標的としたアクセスの増加
- Linear eMerge E3-Series の脆弱性（CVE-2019-7256）を標的としたアクセスの増加

1 宛先ポート 4567/TCP に対する Mirai ボットの特徴を有するアクセスの増加

警察庁のインターネット定点観測において、令和元年 12 月下旬から宛先ポート 4567/TCP に対するアクセスの増加を観測しました。当該アクセスは、宛先 IP アドレスと TCP シーケンス番号[i] の初期値が一致する Mirai ボットの特徴を有しています（図1）。

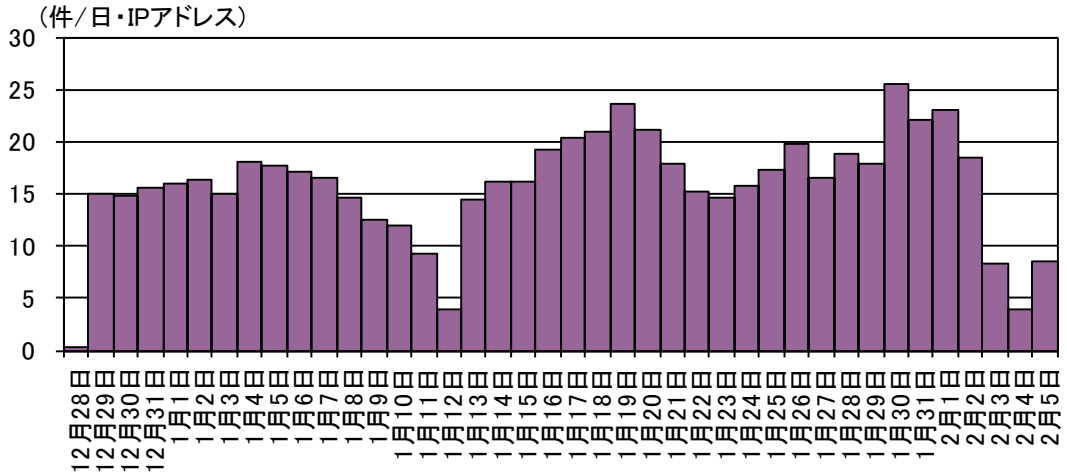

図1 宛先ポート 4567/TCP に対する Mirai ボットの特徴を有する宛先ポート別アクセス件数の推移（R1.12.28～R2.2.5）

観測したアクセスの中には、特定の文字列が含まれており（図2）、海外の共有ウェブサービスにおいて、当該アクセスと関連する PoC [ii] が掲載されていることを確認しております。これらのアクセスは、特定のデジタルビデオレコーダーに対してリモートから文字列を送信することにより、ID とパスワードを窃取することができる脆弱性を悪用したものとみられます。

[i] TCP パケットの送受信状況を管理するための番号で、通常は TCP 通信の開始時にランダムな番号が初期値として設定され、進行に合わせて増加します。また、この初期値を特に ISN（Initial Sequence Number）といいます。
[ii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラム。

図2　観測したアクセスの例（一部マスキング）

また、宛先ポート 4567/TCP に対するアクセスの送信元 IP アドレスを調査したところ、IP カメラや海外製デジタルビデオレコーダー等の IoT 機器のログイン画面が表示されることを確認しました（図3）。

図3　送信元となっている IoT 機器のログイン画面の例

さらに、宛先ポート 4567/TCP に対するアクセスの同一の送信元 IP アドレスからは、23/TCP、80/TCP、8080/TCP 等を宛先ポートとするアクセスも観測しています（図４）。

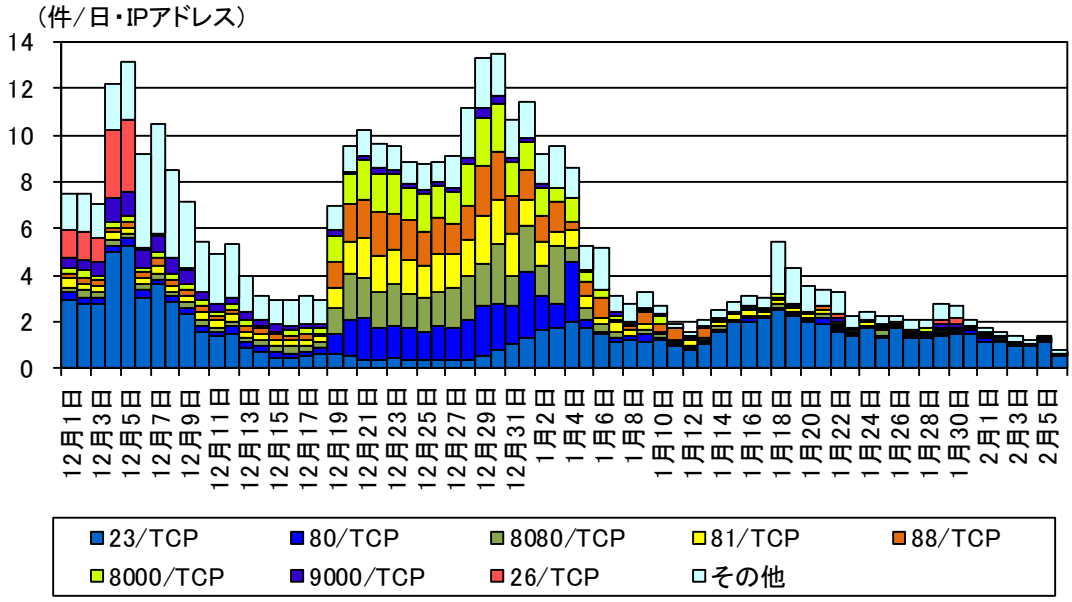

図4　宛先ポート 4567/TCP に対するアクセスの送信元 IP アドレスからの
他の宛先ポートへのアクセス件数の推移（R1.12.1～R2.2.5）

このことから、不正プログラムに感染したボットが感染拡大を意図して、宛先ポート 4567/TCP を使用する IoT 機器を感染対象にしているものと考えられます。

IoT 機器の利用者は、以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- 製品によっては、ファームウェアの自動アップデート機能が存在するものもあります。このような製品を使用している場合には、同機能を有効にしてください。
- IoT 機器をインターネットに接続する場合には、直接インターネットに接続せずに、ルータ等を使用してください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な IP アドレスのみにアクセスを許可する、VPN を用いて接続することも検討してください。
- ユーザ名及びパスワードは初期設定のままで使用せず、必ず変更してください。また、ユーザ名及びパスワードを変更する際は、推測されにくいものにしてください。
- 製造終了から年月が経過した製品は、製造元のサポートが終了し、脆弱性への対応が実施されない場合があります。そのような製品を使っている場合には、サポート中の製品への更新を推奨します。

2　PJL(Printer Job Language)に対応した機器を標的としたアクセスの増加

警察庁のインターネット定点観測において、令和2年1月中旬からPJL(Printer Job Language)を標的とした探索行為と思料されるアクセスの増加を観測しました(図5)。PJL は、ヒューレット・パッカード社によって策定されたプリンタのジョブ制御を行う言語であり、ヒューレット・パッカード社以外のプリンタでも対応しているものがあります。

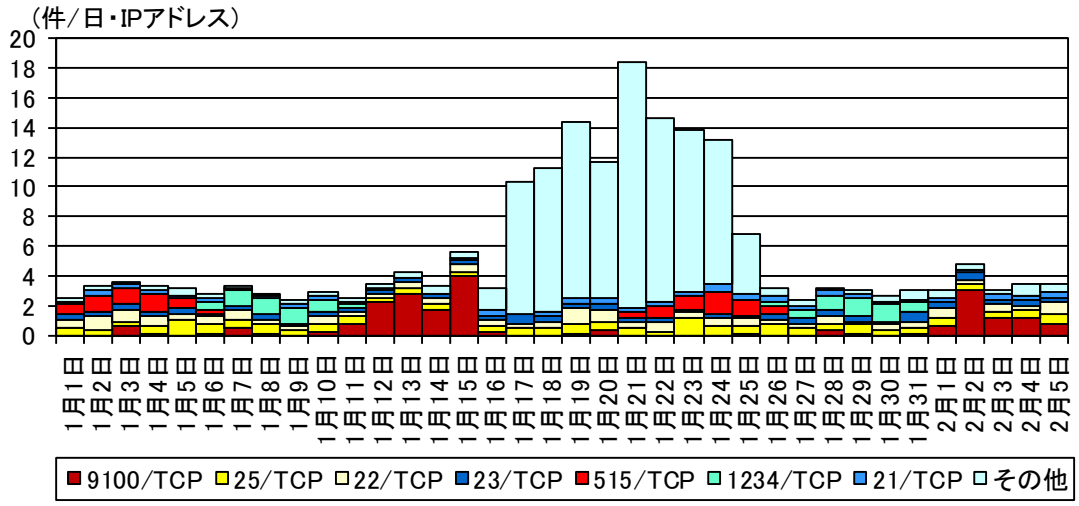

図5　PJL に応答する機器を標的としたアクセス行為の推移(R2.1.1～2.5)

観測したアクセスは、プリンタ等の情報を要求するものや設定の変更を試みるものでした(図6)。

図6　観測したアクセスの例(一部マスキングを実施)

PJL を使用することで、プリンタのジョブの追加、キューの削除を行うことができ、印刷用紙の設定等も行えます。しかし、IPA(情報処理推進機構)の報告書[i]によると、PJL を悪用することにより、プリンタの設定や印刷したデータ等を不正に取得、あるいはプリンタ内に記録されているデータを改ざんすることも可能であると指摘されています。

PJL に対応したプリンタや複合機を使用している場合には、以下の対策を実施することを推奨します。

- インターネットからプリンタや複合機へアクセスできないようにファイアウォールやルータの設定を変更してください。
- インターネットからのアクセスを許可する場合は、必要なIPアドレスのみにアクセスを許可したり、VPN を用いて接続したりすることも検討してください。

[i] 「デジタル複合機のセキュリティに関する調査報告書」
https://www.ipa.go.jp/files/000027285.pdf

3　Linear eMerge E3-Series の脆弱性（CVE-2019-7256）を標的としたアクセスの増加

Linear eMerge E3-Series は、Nortek 社が提供するアクセスコントロールプラットフォームで、部屋の入退室を管理するドアシステム等で利用されています。令和元年7月2日、Linear eMerge E3-Series に存在する深刻な脆弱性（CVE-2019-7256）[i] が公表されました。

当該脆弱性が悪用された場合、攻撃者により遠隔から任意の OS コマンドを実行される可能性があります。また、海外の共有ウェブサービスにおいて、当該脆弱性を対象とした PoC が公開されていることを確認しました。

警察庁のインターネット定点観測において、令和2年1月9日以降、当該脆弱性を標的としたアクセスの増加を観測しました（図6）。

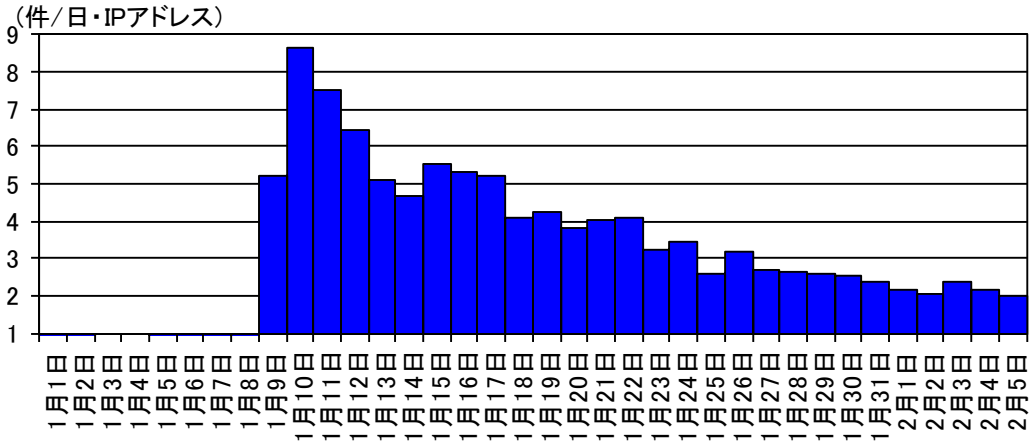

図6　宛先ポート 80/TCP に対する Linear eMerge E3-Series の脆弱性（CVE-2019-7256）を標的としたアクセスの推移（R2.1.1～2.5）

当該アクセスは、Linear eMerge E3-Series の脆弱性を悪用して OS コマンドを実行させることで、外部サーバから不正プログラムのダウンロード及び実行を試みるものでした（図7）。当該不正プログラムは Mirai、またはその亜種とみられます。

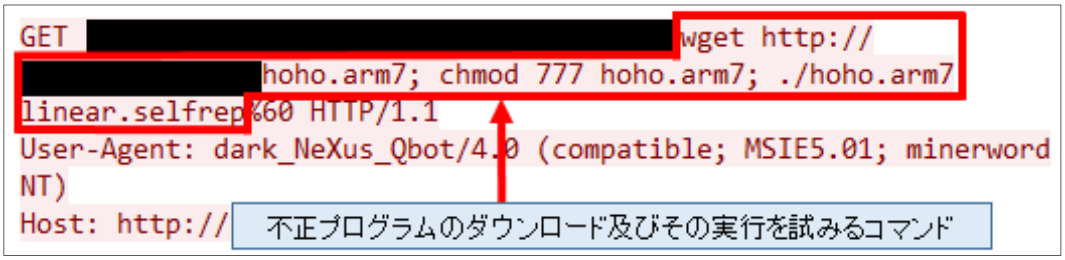

図7　観測したアクセスの例（一部マスキングを実施）

[i] 「CVE-2019-7256 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2019-7256

また、当該アクセスの同一の送信元 IP アドレスからは、60001/TCP、23/TCP 等を宛先ポートとするアクセスも観測しており、不正プログラムに感染したボットが新たな標的を追加し、感染活動を活発化させ始めたものとみられます。

管理する機器が Linear eMerge E3-Series を利用している場合には、以下の対策を実施することを推奨します。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な IP アドレスのみにアクセスを許可したり、VPN を用いて接続したりすることも検討してください。
- 必要がない限りは、インターネットからのアクセスを無効にしてください。