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

平成 27 年 10 月 28 日

インターネット観測結果等

（平成 27 年9月期）

- Linux が組み込まれている機器を発信元とした宛先ポート 23/TCP に対するアクセスが増加
- マルウェアに感染した Cisco 社製ルータの探索と考えられるアクセスを観測

1　Linux が組み込まれている機器を発信元とした宛先ポート 23/TCP に対するアクセスが増加

警察庁の定点観測システムでは、23/TCP を宛先ポートとするアクセスが継続的に増加していることを観測しました（図 1）。

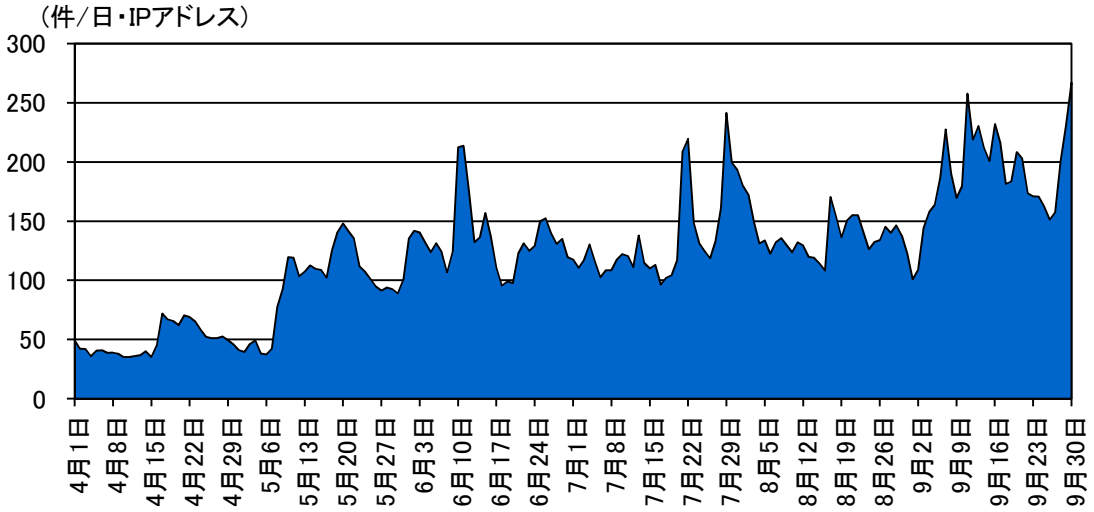

図 1　宛先ポート 23/TCP に対するアクセス件数の推移（H27.4.1～9.30）

23/TCP は、Telnet で使用されるポートであり、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に行われていると考えられます。これらのアクセスを確認したところ、センサー到達時の TTL(Time To Live)値が 64 以下のものが 98.6%を占めていました（図 2）。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。これにより、当該アクセスについては Linux 系の OS が組み込まれた機器が発信元である可能性が高いと考えられます。

Linux は、組み込み OS の分野において過半数のシェアを占め、スマートフォン、ネットワーク機器、デジタル家庭電化製品といった IoT(Internet of Things ： モノのインターネット)機器の OS として広く普及しています[i]。

---

[i] 「Embedded Linux Keeps Growing Amid IoT Disruption, Says Study」（平成 27 年3月 20 日）
http://www.linux.com/news/embedded-mobile/mobile-linux/818011-embedded-linux-keeps-growing-amid-iot-disruption-says-study

当該アクセスの発信元を調査したところ、ウェブカメラ、ネットワークストレージ、デジタルビデオレコーダー等の特徴が見られることから、IoT 機器が攻撃者に乗っ取られ、攻撃の踏み台等に悪用されている可能性があります。

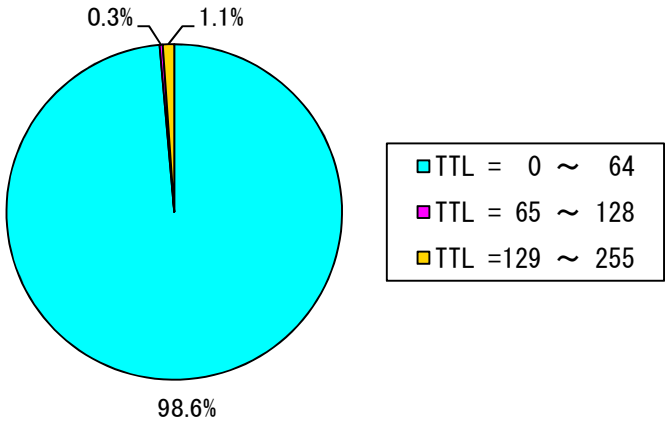

図 2　宛先ポート 23/TCP に対するアクセスにおける TTL 値の内訳

2　マルウェアに感染した Cisco 社製ルータの探索と考えられるアクセスを観測

平成 27 年9月 20 日に、マルウェアに感染した Cisco 社製ルータの探索と考えられるアクセスについて注意喚起を実施[i]していますが、その後も同様のアクセスを継続して観測しています。

16 日から始まったミシガン大学が管理する IP アドレスからのアクセスは 26 日まで継続し、17 日から始まった特定の非営利組織[ii]（以下「非営利組織 1」という。）が管理する IP アドレスからのアクセスは現在も継続しているほか、22 日から 23 日の間には別の非営利組織（以下「非営利組織 2」という。）が管理する IP アドレスからのアクセスを観測しました。また、18 日から 25 日の間にはこれらの組織が管理する IP アドレスとは異なる IP アドレスからの探索活動を観測しました（図 3）。

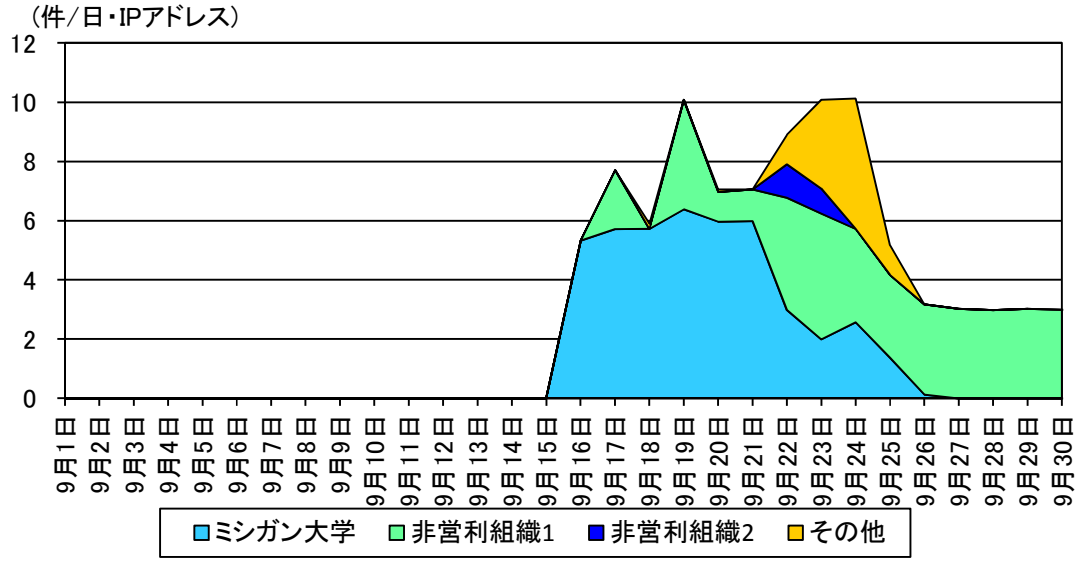

図 3　マルウェアに感染した Cisco 社製ルータの探索と考えられるアクセス件数の推移
（発信元グループ別）（H27.9.1～9.30）

これらのミシガン大学、非営利組織1及び非営利組織2によるもの以外のアクセスについては、インターネットサービスプロバイダやホスティングサービス事業者が管理する海外の国に割り当てられたIPアドレスが発信元であり、探索行為の実施者や目的が不明であることから、一部のセキュリティ対策企業では、マルウェアによって作成されたバックドアを悪用して、ルータに不正なアクセスを試みようとする攻撃者が、探索活動を実施している可能性も考えられるとしています。また、マルウェアの詳細について公表したセキュリティ対策企業は、マルウェアの感染経路の断定には至っていないながらも、次の2点が原因として考えられるとしています。

---

[i] 「マルウェアに感染した Cisco 社製ルータを探索するアクセスの観測について」（平成 27 年9月 20 日）
https://www.npa.go.jp/cyberpolice/topics/?seq=16930

[ii] インターネットセキュリティの向上を目的として、攻撃を受ける可能性があるサービスが稼動している IP アドレスの探索等の活動を実施している非営利組織。探索結果は、当該 IP アドレス帯域の管理者等に限定して公開されている。

- ルータの管理用パスワードを初期値のまま使用している。
- ルータの管理用パスワードが何らかの方法で漏えいした。

これらのことから、ルータ等のネットワーク機器においても、設定しているパスワードや、その管理方法について再度点検を実施することを推奨します。