平成 29 年3月 22 日

不正プログラムに感染した IoT 機器が発信元と考えられるアクセスの増加等について

- 不正プログラムに感染した IoT 機器が発信元と考えられるアクセスの増加
  - ・宛先ポート 5358/TCP に対するアクセスの急増
  - ・宛先ポート 32/TCP 及び 3232/TCP に対するアクセスの急増
  - ・宛先ポート 19058/TCP に対するアクセスの急増
- NETGEAR 製ルータの脆弱性を標的としたアクセスを観測

1 不正プログラムに感染した IoT 機器が発信元と考えられるアクセスの増加について

(1) 宛先ポート 5358/TCP に対するアクセスの急増

インターネット定点観測システムでは、1月下旬頃から宛先ポート 5358/TCP に対するアクセスの急増を観測しました(図1)。

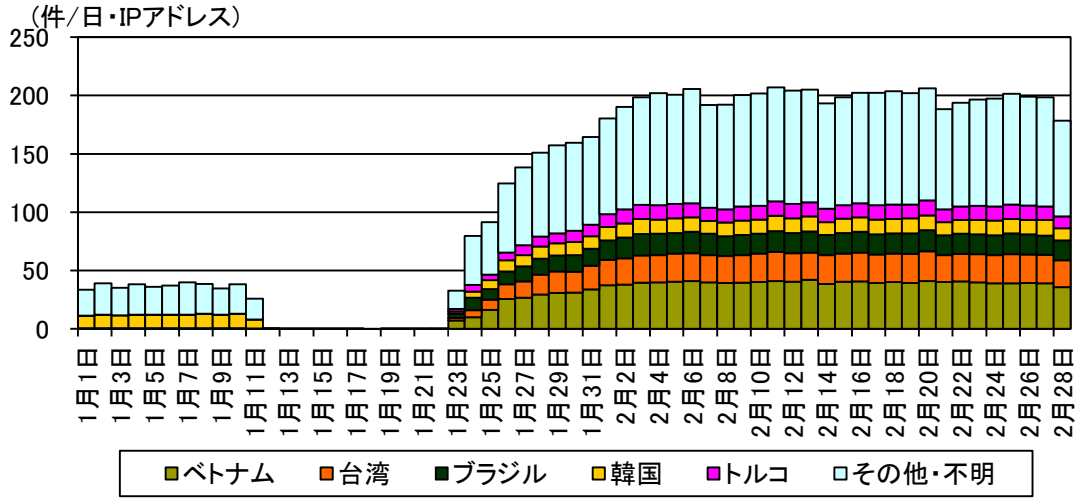

図1 宛先ポート 5358/TCP に対するアクセス件数の発信元国・地域別推移[i] (H29.1.1～2.28)

これらのアクセスを確認したところ、宛先ポート 23/TCP に対してもアクセスをしている発信元 IP アドレスが約 52%存在しており、それらの発信元 IP アドレスに対して、ウェブブラウザを使用して接続したところ、ネットワークカメラ、ルータ等のネットワーク機器のログイン画面が表示されることを確認しました。

[i] 発信元の国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。

また、これらのアクセスには、「Mirai」ボットの特徴[i]の一つとされている宛先 IP アドレスと TCP シーケンス番号[ii]の一致はみられなかったことから、観測したアクセスは「Mirai」ボットとは異なる不正プログラムに感染した IoT 機器からのアクセスである可能性が考えられます。

(2) 宛先ポート 32/TCP 及び 3232/TCP に対するアクセスの急増

インターネット定点観測システムでは、2月6日から宛先ポート 32/TCP 及び 3232/TCP に対するアクセスの急増を観測しました(図2)。これらのアクセスを確認したところ、TCP シーケンス番号と宛先 IP アドレスが一致した「Mirai」ボットの特徴がみられるアクセスが 99%以上を占めていました。(図3及び図4)。

また、TCP シーケンス番号と宛先 IP アドレスが一致したアクセスの件数の割合を比較したところ、おおむね1対1であり、宛先ポート 23/TCP 及び 2323/TCP に対する「Mirai」ボットのアクセスの比率である9対1[iii]とは異なりました。

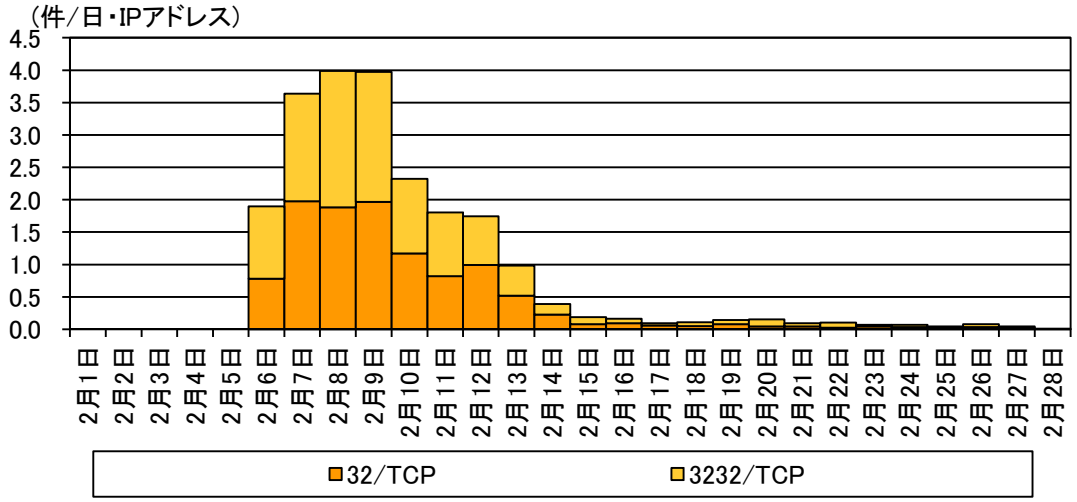

図2 宛先ポート 32/TCP 及び 3232/TCP に対するアクセス件数の推移

[i] 「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について
http://www.npa.go.jp/cyberpolice/important/2017/19824.html

[ii] TCP シーケンス番号は、TCP パケットの送受信状況を管理するために付与される番号です。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、TCP 通信の進行に合わせて増加していきます。

[iii] インターネット観測結果等(平成 28 年9月期)
http://www.npa.go.jp/cyberpolice/important/2016/19361.html

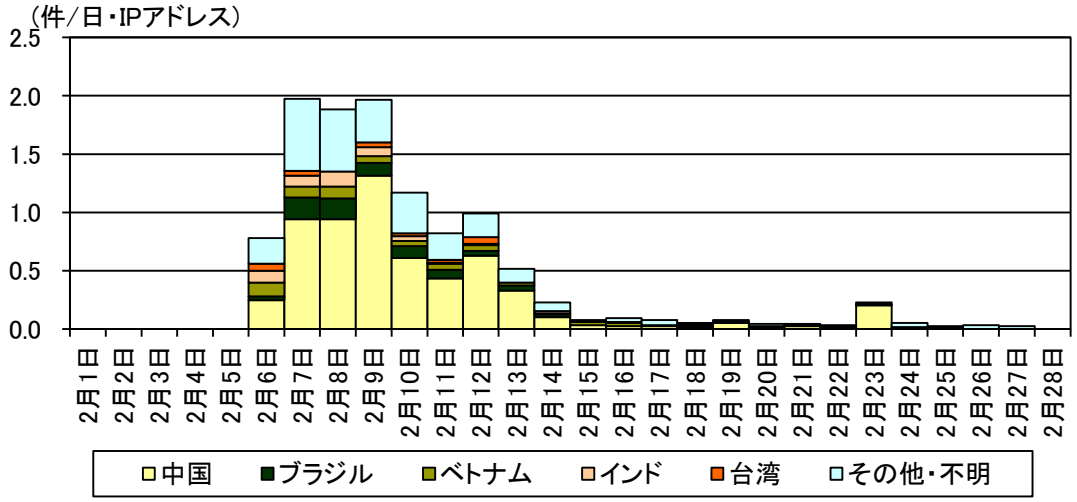

図3　宛先ポート 32/TCP に対するアクセス件数の発信元国・地域別推移
（TCP シーケンス番号と宛先 IP アドレスが一致するアクセスのみ）

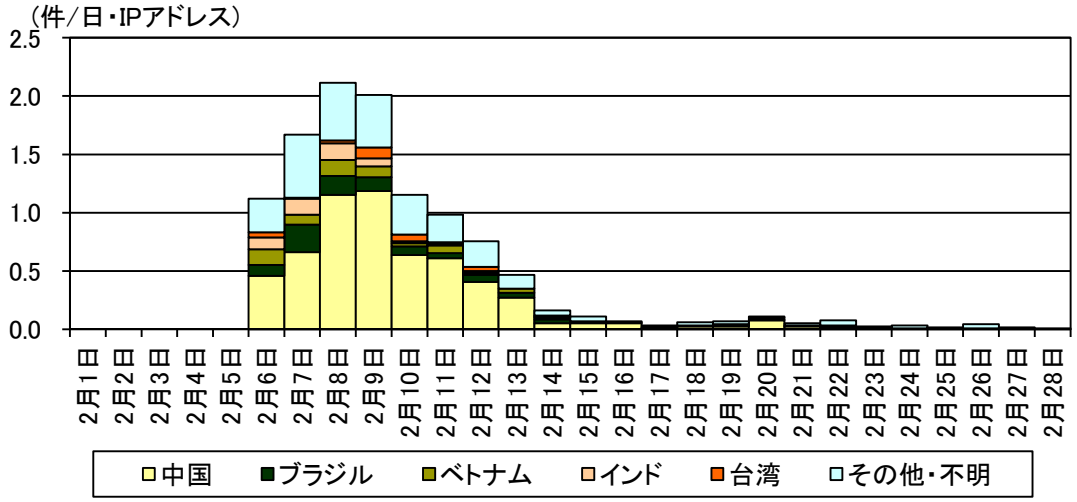

図4　宛先ポート 3232/TCP に対するアクセス件数の発信元国・地域別推移
（TCP シーケンス番号と宛先 IP アドレスが一致するアクセスのみ）

宛先ポート 32/TCP 及び 3232/TCP に対するアクセスの発信元 IP アドレスからパケットの送信状況を確認すると、23/TCP、2323/TCP にも TCP シーケンス番号と宛先 IP アドレスが一致した「Mirai」ボットの特徴を持つパケットを送信していました。

さらに、発信元 IP アドレスに対して、ウェブブラウザを使用して接続したところ、ネットワークカメラ、ルータ等のネットワーク機器のログイン画面が表示されることを確認しました。

以上のことから、これらのアクセスの急増は、「Mirai」ボットの亜種による宛先ポート 32/TCP 及び 3232/TCP を標的としたアクセスの可能性が考えられます。

(3) 宛先ポート 19058/TCP に対するアクセスの急増

インターネット定点観測システムでは、2月3日頃から宛先ポート 19058/TCP に対するアクセスの急増を確認しました(図5)。

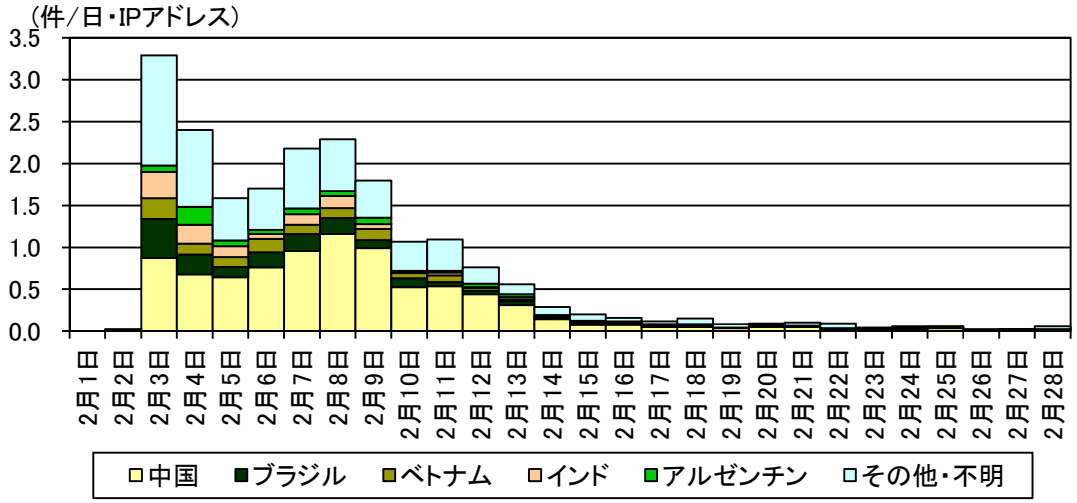

図5 宛先ポート 19058/TCP に対するアクセス件数の発信元国・地域別推移

これらのアクセスを確認したところ、TCP シーケンス番号と宛先 IP アドレスが一致した「Mirai」ボットの特徴がみられるアクセスが 99%以上を占めており、これらの発信元 IP アドレスの送信状況を確認したところ、宛先ポート 23/TCP、2323/TCP にも TCP シーケンス番号と宛先 IP アドレスが一致した「Mirai」ボットの特徴を持つパケットを送信していました。また、12 月 18 日からアクセスの急増を観測している宛先ポート 6789/TCP のパケットにおいて、宛先ポート 19058/TCP にバックドア [i] の構築を企図していると考えられるアクセスを観測 [ii] しています。

さらに、発信元に対して、ウェブブラウザを使用して接続したところ、ネットワークカメラ、ルータ等のネットワーク機器のログイン画面が表示されることを確認しました。

以上のことから、このアクセスの急増は、「Mirai」ボットの亜種のによる宛先ポート 19058/TCP のバックドアを標的としたアクセスの可能性が考えられます。

---

[i] コンピュータに設けられた通信経路のうち、正規の経路や手段を経ずにシステムへ侵入するために設けられる接続経路。

[ii] 「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について
http://www.npa.go.jp/cyberpolice/important/2017/19824.html

(4) IoT 機器を守るために推奨する対策

IoT 機器を対象とした「Mirai」等のボットは巨大なボットネットを作成するため、さまざまな機器の脆弱性や設定の不備を悪用し、感染を拡大させていきます。特に「Mirai」ボットが標的としていた Linux が動作している IoT 機器だけでなく、それ以外の OS が動作している機器を標的としたボットも作成されているとの報告[i]があるところです。

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。

- 初期設定のユーザ名及びパスワードのままでは使用せず、ユーザ名とパスワードを推測されにくいものに変更してください。
- 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。また、ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。
- 製造元のウェブサイト等で脆弱性情報を確認し、脆弱性がある場合はファームウェアのアップデート等の適切な対策を行ってください。

[i] 「ポートスキャン機能を増強した「Mirai」、Windows も踏み台に追加」
http://blog.trendmicro.co.jp/archives/14455

2 NETGEAR 製ルータの脆弱性を標的としたアクセスを観測

平成 28 年 12 月 9 日に、米国の CERT/CC から複数の NETGEAR 製無線 LAN ルータにおいて重大な脆弱性が存在することが公表[i]されました。また、12 月 12 日には JVN から同脆弱性に関する情報が国内向けに公表[ii]されています。公表された情報によると、当該脆弱性が悪用された場合、ルータ上で遠隔から任意のコードを実行させることが可能であるとされています。

インターネット定点観測システムにおいては、平成 29 年2月 27 日に、同脆弱性を悪用していると考えられる宛先ポート 80/TCP に対するアクセスを観測しました(図6)。

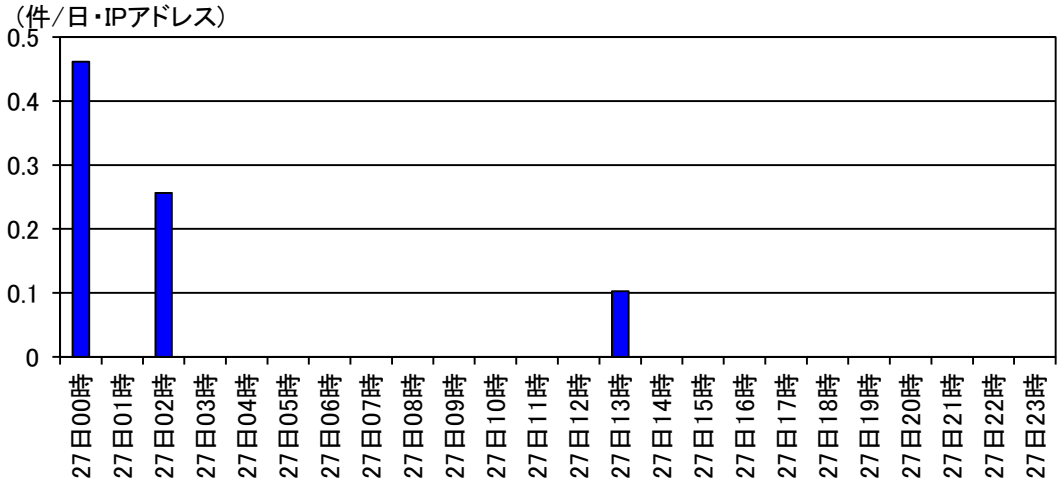

図6 NETGEAR 製ルータの脆弱性を標的としたアクセス件数の推移(2月 27 日)

観測したアクセスに含まれていたコードは全て外部からファイルのダウンロード及び実行を試みるものでした(図7)。同アクセスの内容から、脆弱性の存在する NETGEAR 製ルータを何らかの不正プログラムに感染させる意図があるものと考えられます。

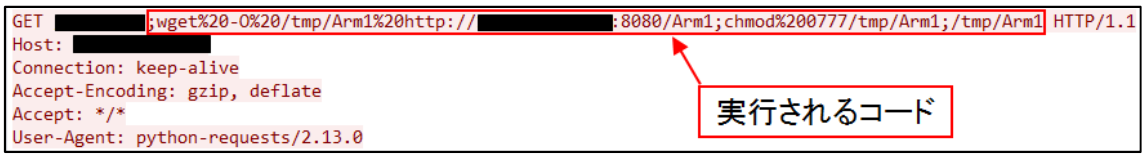

図 7 観測したアクセスのリクエスト内容(一部マスキングを実施)

同ルータの初期設定では、当該脆弱性が存在する管理画面はプライベートネットワーク側からのみアクセスできる状態であるため、インターネット側から当該脆弱性を悪用することはできません。しかしながら、リモート管理機能が有効であり、かつアクセス制限が適切に設

[i] Vulnerability Note VU#582384 Multiple Netgear routers are vulnerable to arbitrary command injection
https://www.kb.cert.org/vuls/id/582384

[ii] JVNVU#94858949 複数の NETGEAR 製ルータに脆弱性
http://jvn.jp/vu/JVNVU94858949/

定されていない場合は、同画面にインターネット側からもアクセスできるようになるため、遠隔から任意のコードを実行させることが可能となります。また、ゲストネットワークをパスワードなしで使用しており、かつ同ネットワークからプライベートネットワークへのアクセスを許可している場合は、ゲストネットワークを経由してプライベートネットワーク側から直接当該脆弱性を悪用することができるので注意が必要です(図8)。

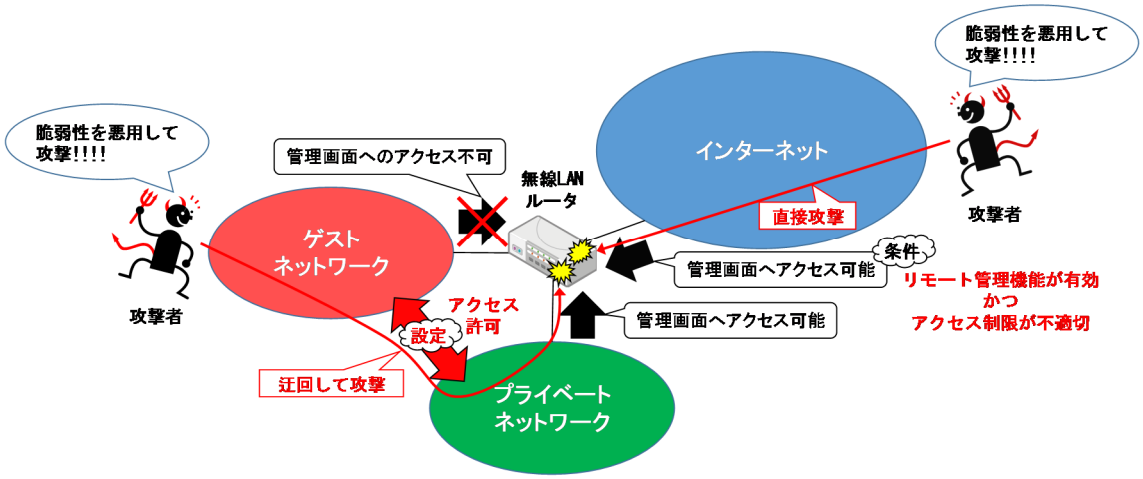

図8　脆弱性を悪用した攻撃のイメージ

NETGEAR 製のルータを使用している場合は以下の対策を実施することを推奨します。

- 製造元の情報 [i] を参考に、使用しているルータが当該脆弱性の影響を受ける製品ではないか確認を実施してください。
- 使用しているルータが当該脆弱性の影響を受ける製品であった場合は、対策済みの最新のファームウェアにアップデートしてください。
- リモート管理機能を有効にする必要がある場合は、アクセス制限を適切に設定してください。
- ゲストネットワークを使用する必要がある場合は、パスワードを適切に設定するとともに、プライベートネットワークへのアクセスの可否について検討してください。

[i] 【更新】【重要】NETGEAR 製ルータにコマンドインジェクションの脆弱性について
https://www.netgear.jp/supportInfo/NewSupportList/174.html