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

平成 27 年5月 25 日

Topic

特定のポートを対象としたプロキシ探索の増加について

特定のポート(37564/TCP)を対象としたプロキシ探索のアクセスが増加しています。攻撃者が攻撃の踏み台として悪用するために、外部からのアクセス制限が行われていないオープンプロキシを探索していると考えられます。また、この探索は、オンラインゲームのユーティリティツールを導入している一般のコンピュータを標的としている可能性があることから、対策を実施することを推奨します。

1 宛先ポート 37564/TCP に対するアクセスの増加

宛先ポート 37564/TCP に対するアクセスが、5月中旬以降増加しています(図1)。

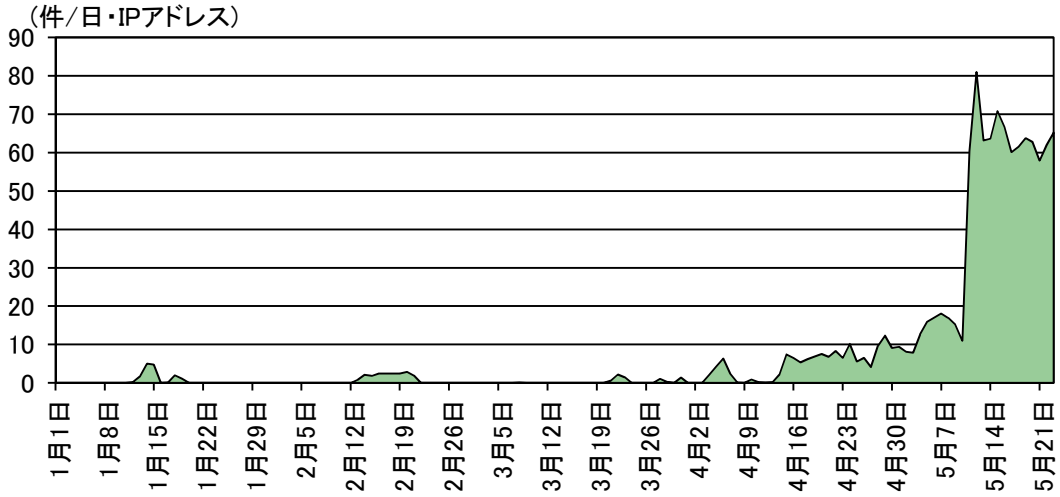

図1 宛先ポート 37564/TCP に対するアクセス件数の推移

このポートに対するアクセスには、接続先のコンピュータがインターネット接続を中継する「プロキシ」として動作するかどうかの確認を行っているものが多く見られました。攻撃者が、外部から利用可能なプロキシを探索する目的でアクセスを行っていると考えられます。

2 踏み台となるオンラインゲームのユーティリティツールの確認

国内オンラインゲームのユーティリティツールが初期設定でプロキシとして使用するポートが37564/TCP であることを確認しています。

当該ツールは、特定のオンラインゲームの動作を監視して、ゲームの進行状況等を確認しやすくするためのソフトウェアであり、当該ツールの利用者は、使用するコンピュータ上でこれを起動してオンラインゲームにアクセスします。また、当該ツールは、プロキシとして動作する機能を有しており、外部からのアクセス制限が行われない場合、外部から利用できる「オープンプロキシ」として動作することを確認しています。

このアクセスは、外部からのアクセス制限が行われていない環境で当該ツールが起動しているコンピュータを標的として、プロキシの探索を行っている可能性があります。

3 推奨する対策

使用するコンピュータが、オープンプロキシとして動作していた場合、攻撃者に攻撃の踏み台として悪用される危険性があります。

起動するだけでプロキシとして機能するソフトウェアもあり、意図せず、使用するコンピュータがプロキシとして動作している可能性があります。こういったソフトウェアを利用する場合に限らず、使用するコンピュータをインターネットに接続する場合は、以下の対策を実施することを推奨します。

- ルータや OS のファイアウォール等の機能により外部からのアクセス制限を行う。
- 不用意に OS のファイアウォール機能を停止させない。