平成 27 年6月 24 日

インターネット観測結果等

（平成 27 年5月期）

- プロキシで使用されるポートに対するアクセスが増加
- Elasticsearch の新たな脆弱性を標的としたアクセスを観測
- 乗っ取られたネットワーク機器による Telnet 探索が増加

1 プロキシで使用されるポートに対するアクセスが増加

今期は、プロキシで使用される様々なポートに対するアクセスの増加を観測しました。プロキシで使用される宛先ポートのうち検知件数が多かったものは、次のとおりです（図1、表1）。

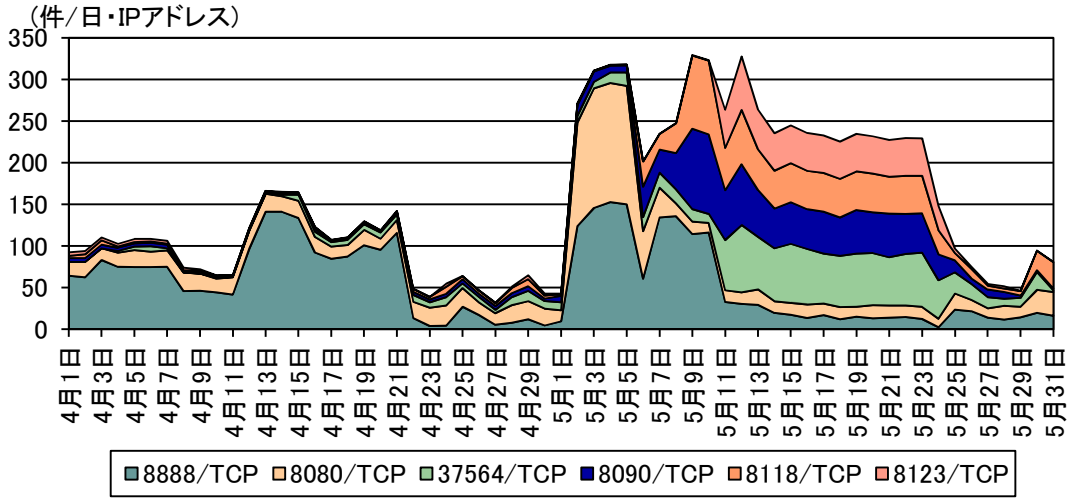

図1 プロキシで使用される主な宛先ポートに対するアクセス件数の推移（H27.4.1～5.31）

表1 プロキシで使用される主な宛先ポートに対するアクセス件数

今期順位[i]	ポート	今期件数[ii]	当該ポートを使用するサービス等
3 位	8888/TCP	48.45 件	プロキシソフト「Fiddler」で使用するポート。
5 位	37564/TCP	36.06 件	オンラインゲームユーティリティツールで使用するポート。
6 位	8090/TCP	35.70 件	プロキシで使用される代表的なポート。8080/TCP の代替として利用される。
7 位	8080/TCP	33.27 件	プロキシで使用される代表的なポート。
8 位	8118/TCP	32.63 件	プロキシソフト「Privoxy」で使用するポート。
10 位	8123/TCP	21.10 件	プロキシソフト「Polipo」で使用するポート。

[i] センサーに対するアクセスを宛先ポート別に集計した検知件数順位。
[ii] 一日・1IP アドレス当たり。

いずれのポートでも、プロキシとして動作するかどうかを試行するアクセスが確認されており、外部から利用可能なオープンプロキシを探索することを目的としたアクセスであると考えられます（図2）。

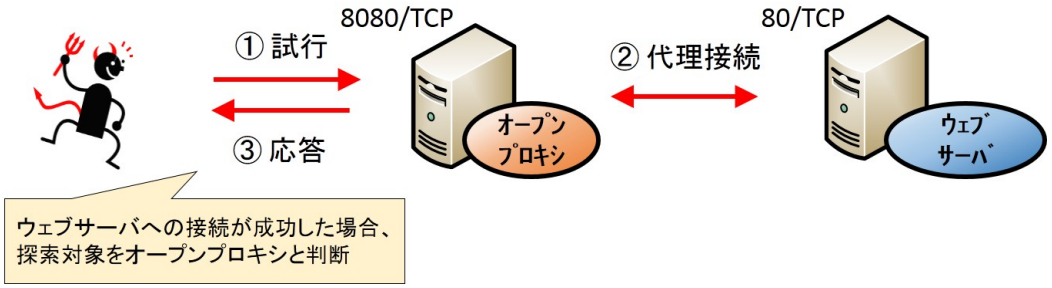

図2　オープンプロキシの探索を目的としたアクセス

プロキシは、攻撃者の発信元IPアドレスを匿名化するなどの特徴があり、外部から利用可能であるオープンプロキシは、攻撃の踏み台として悪用される危険性があります。

1-1 プロキシサーバを対象とした探索

8080/TCP や 8090/TCP については、プロキシサーバで利用されることが多いポートであり、探索の対象はこれらプロキシサーバであると考えられます。通常、プロキシサーバは、組織内部から利用する目的で設置し、外部からのアクセス制限が行われます。これらの探索は、設定の不備等によりオープンプロキシとして動作しているサーバを探索しているものと考えられます。

1-2 一般のコンピュータを対象とした探索

8888/TCP、37564/TCP、8118/TCP及び8123/TCPについては、個人が使用する一般のコンピュータ上で稼動するプロキシソフト等が初期設定で使用するポートであり、攻撃者は、これら一般のコンピュータで稼動しているプロキシを探索の対象としている可能性があります。これら一般のコンピュータで稼動するプロキシは、プロキシサーバとして運用されているものとは異なり、適切にログが管理されていないため悪用した証跡が残りにくく、より匿名性の高い攻撃の踏み台として攻撃者に悪用される危険性があります。

特に、宛先ポート 37564/TCP に対するアクセスは、国内オンラインゲームのユーティリティツールを対象とした探索と考えられるものであり、国内に多数の利用者が存在すると考えられたことから、別途、注意喚起を実施しています[i]。

[i] 「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」（平成 27 年5月 25 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=16375

2 Elasticsearch の新たな脆弱性を標的としたアクセスを観測

平成27年3月、オープンソースの全文検索システムElasticsearchで使用されるポート9200/TCPに対するアクセスが増加しましたが[i]、このポートに対するアクセスを継続して観測しています(図3)。

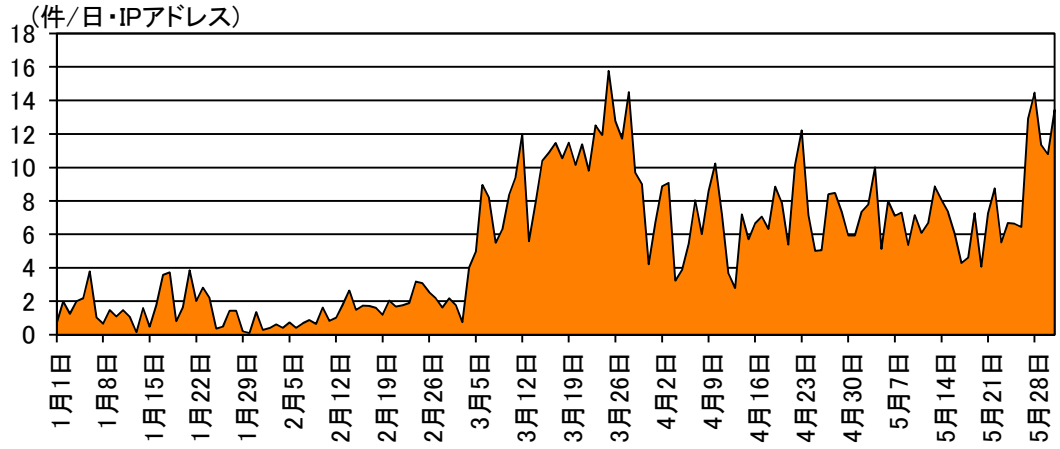

図3 宛先ポート9200/TCPに対するアクセス件数の推移(H27.1.1～5.31)

3月以降、Elasticsearchの脆弱性を標的としたアクセスを観測してきたましたが[ii]、4月 27 日には、Elasticsearch に新たな脆弱性が存在することが公表され[iii]、当該脆弱性を標的としたものと考えられるアクセスも観測しています(図4)。

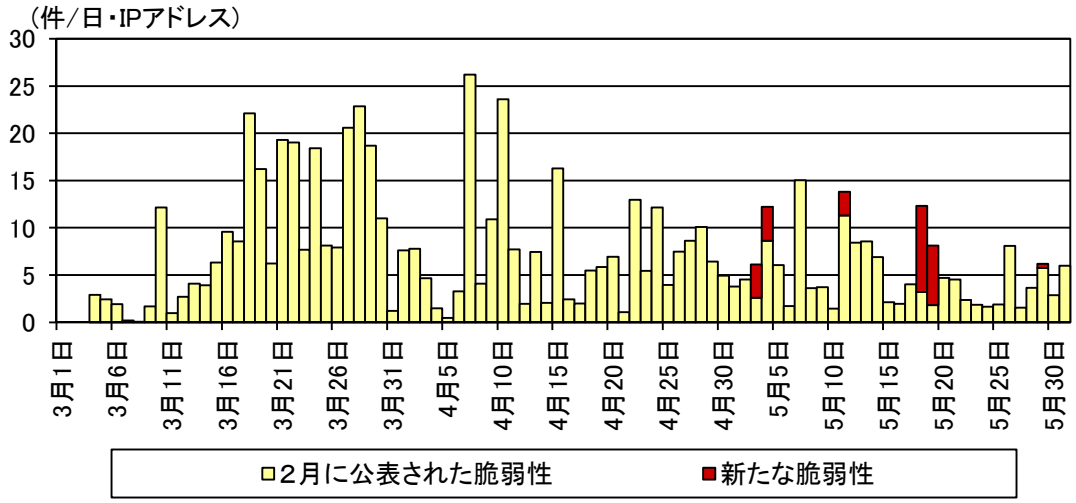

図4 Elasticsearchの脆弱性を標的としたもの考えられるアクセスの推移(H27.3.1～5.31)

[i] 「インターネット観測結果等(平成27年3月期)」(平成27年5月7日)
http://www.npa.go.jp/cyberpolice/topics/?seq=16261
[ii] 「Elasticsearchの脆弱性を標的としたアクセスの観測について」(平成27年3月16日)
http://www.npa.go.jp/cyberpolice/topics/?seq=15728
[iii] 「Elasticsearchにおけるディレクトリトラバーサルの脆弱性」
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002536.html

Elasticsearch を使用している場合は、ベンダからの情報[i]を参考にして、バージョンアップや設定の変更等を行うことを推奨します。また、不審なファイルが存在しないか、不正なアクセスが行われていないかなどの確認を行うことも大切です。

3　乗っ取られたネットワーク機器からの Telnet 探索が増加

今期は、宛先ポート 23/TCP に対するアクセスの増加を観測しました（図5）。

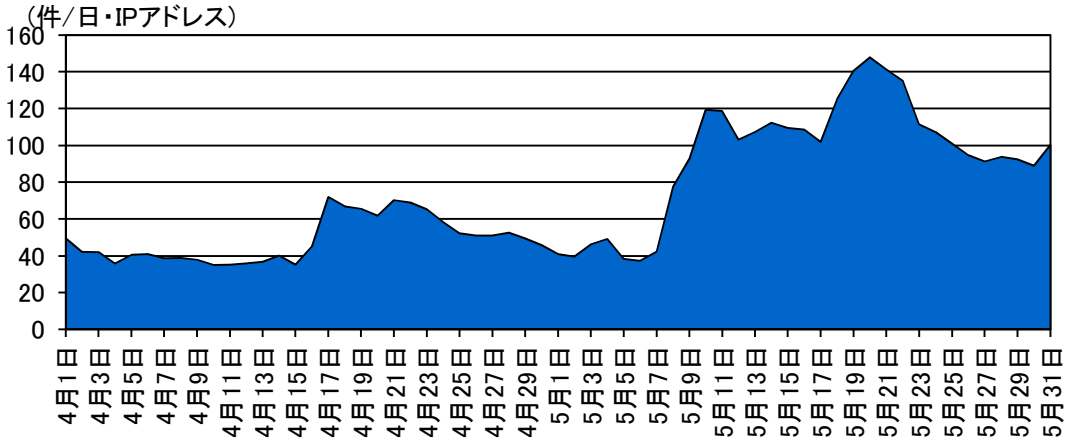

図5　宛先ポート 23/TCP に対するアクセス（H27.4.1～5.31）

このポートは Telnet で使用されるものであり、Telnet でログイン可能なコンピュータやネットワーク機器を探索する目的で行われていると考えられます。これらのアクセスの発信元を調査したところ、DVR（デジタルビデオレコーダ）、ウェブカメラ及びルータ等のネットワーク機器の特徴が見られたことから、これらネットワーク機器が攻撃者に乗っ取られ、探索行為を行っているものと考えられます。

これらネットワーク機器は、攻撃者の命令に基づいて動作するボットとして動作していると考えられ、ボットの感染拡大を目的として Telnet 探索を行っている可能性があります（図6）。

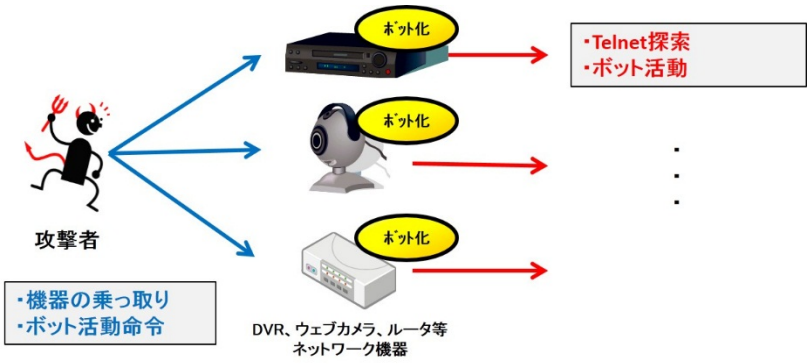

図6　ネットワーク機器のボット化

[i] 「Elasticsearch 1.5.2 and 1.4.5 Released」
https://www.elastic.co/blog/elasticsearch-1-5-2-and-1-4-5-released