平成 27 年5月 7日

インターネット観測結果等

（平成 27 年3月期）

- Elasticsearch の脆弱性を標的としたアクセスを観測
- 宛先ポート 8888/TCP に対するアクセスが増加
- 発信元ポート 80/TCP からの SYN/ACK パケットが急増

1 Elasticsearch の脆弱性を標的としたアクセスを観測

警察庁の定点観測システムでは、3月上旬以降、宛先ポート 9200/TCP に対するアクセスの増加を観測しました（図1）。9200/TCP はオープンソースの全文検索システム Elasticsearch においてデフォルトで使用されるポートです。

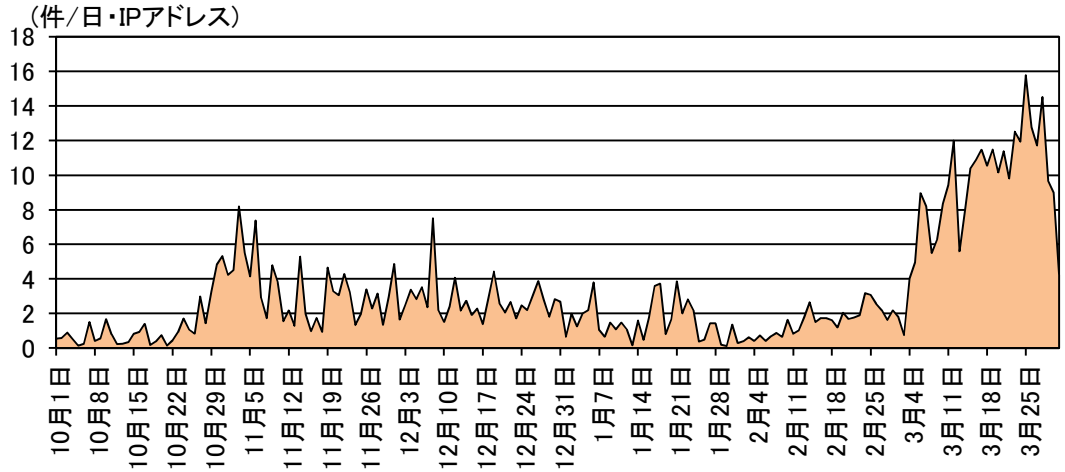

図1 宛先ポート 9200/TCP に対するアクセス件数の推移（H26.10.1～H27.3.31）

Elasticsearch の脆弱性については、2 月 11 日にリモートから任意のコマンドを実行できる脆弱性[i]が公表されました。その後、3月上旬には当該脆弱性を検証するためのプログラム（PoC[ii]）が公開されています。

定点観測システムにおいては、この脆弱性を標的としたと思われるアクセスを観測し、3月 16 日に注意喚起[iii]を行っています。それ以降も、同様のアクセスを継続して観測しています（図2）。

---

i Elasticsearch の Groovy スクリプトエンジンにおけるサンドボックス保護メカニズムを回避される脆弱性（CVE-2015-1427）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001538.html

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のこと。

iii「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/detect/pdf/20150316.pdf

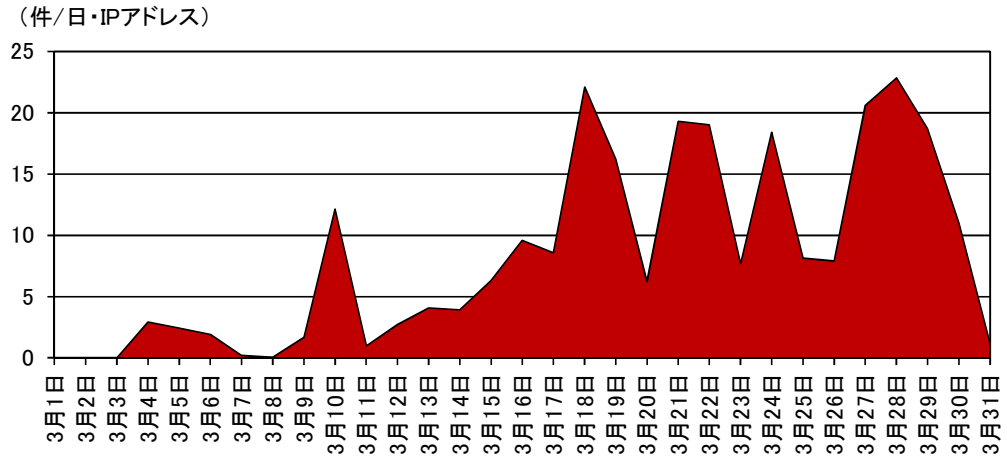

図2　Elasticsearch の脆弱性を標的としたアクセス件数の推移

観測したパケットの内容を確認したところ、OS 情報の取得や外部サーバからの不審なファイルのダウンロード等のコマンドが含まれていました。

不審なファイルについては、指令サーバからの要求に応じて、DoS 攻撃等を行うボットプログラムとして利用されるものであると考えられます。

2　宛先ポート 8888/TCP に対するアクセスが増加

3月中旬から宛先ポート 8888/TCP に対するアクセスの急増を観測しました（図3）。

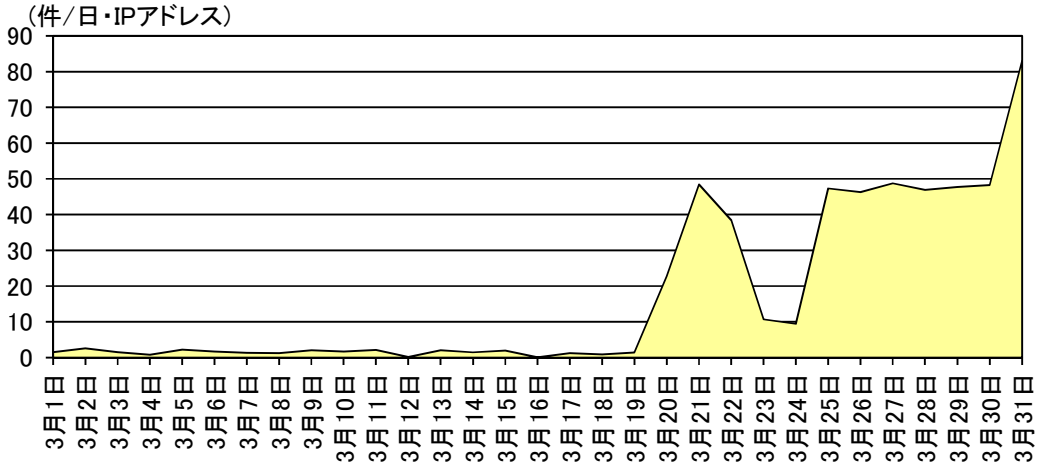

図3　宛先ポート 8888/TCP に対するアクセス件数の推移

観測したパケットの内容を確認したところ、アクセスの多くは対象の機器がポート 8888/TCP への接続要求に応答するか探索を実施しているものであり、その他、外部からプロキシとして利用可能であるか確認するアクセスも存在しました。

３　発信元ポート 80/TCP からの SYN/ACK パケットが急増

３月には発信元ポート 80/TCP からの SYN/ACK パケットの増加を観測しました（図4）。これらのパケットは DoS 攻撃の標的となったウェブサーバからの跳ね返りパケットであると考えられます。

なお、３月期の DoS 攻撃被害観測状況における発信元国・地域別の上位は、カナダ、米国、フランスの順でした。

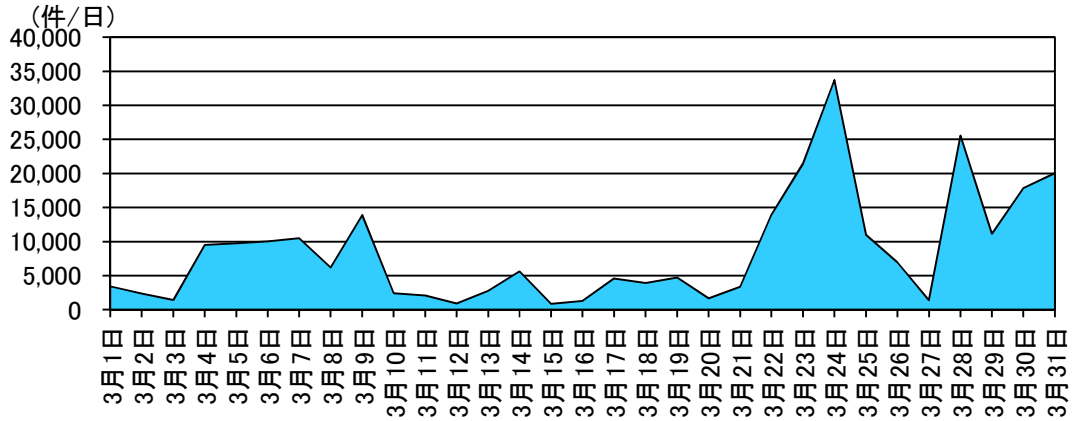

図4　発信元ポート 80/TCP の SYN/ACK パケットの推移