平成 27 年3月 31 日

インターネット観測結果等

（平成 27 年2月期）

- オープン・リゾルバを踏み台とした jp ドメインに対する DDoS 攻撃を観測
- MongoDB データベースに対する探索行為が増加

1 オープン・リゾルバを踏み台とした jp ドメインに対する DDoS 攻撃を観測

オープン・リゾルバに対して、攻撃対象ドメインのランダムなサブドメインの問い合わせを送信することにより、当該ドメインの権威 DNS サーバに問い合わせを集中させ、正常な運用を妨害する DDoS 攻撃手法[i]については、これまでにも注意喚起[ii]を実施してきたところです。同攻撃について初めて観測した平成 26 年以降は、jp ドメインを対象とする攻撃は観測[iii]していませんでした。

しかしながら、2月2日から4日の間に特定の jp ドメインを対象とする攻撃に起因すると考えられるパケットを断続的に観測しました（図1）。

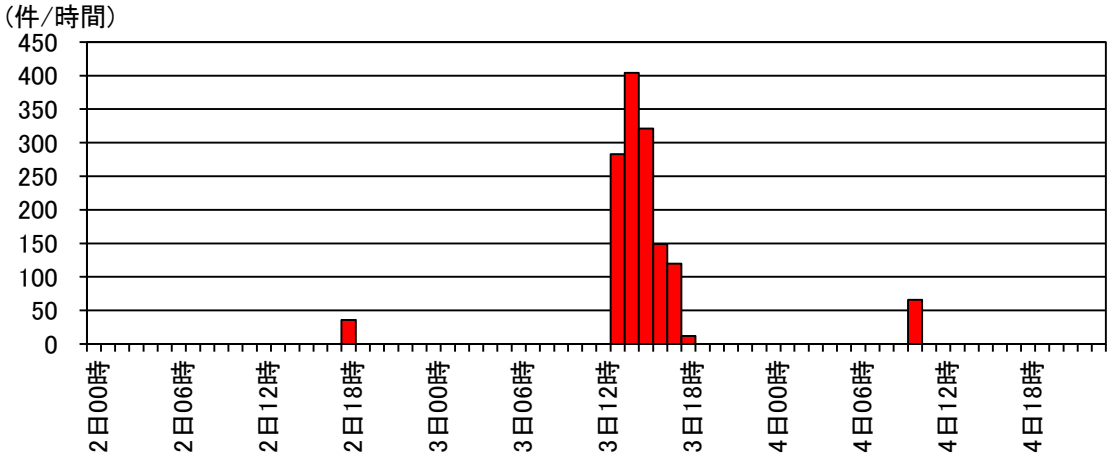

図1 特定の jp ドメインの DNS 回答パケットの観測件数の推移（H27.2.2～2.4）

当該 jp ドメインを所有する組織は、ウェブサイトが大規模なサイバー攻撃を受け、サイト閲覧に支障が生じた旨を明らかにしており、観測されたパケットは同攻撃に起因するものと考えられます。

オープン・リゾルバを踏み台とした jp ドメインに対する攻撃が観測されたのは今回が初めてですが、今後、同攻撃手法が多用されるようになり、日本国内の企業や組織等に対する同種の攻撃が

---

[i] 同攻撃手法については、「DNS 水責め攻撃（Water Torture Attack）」、「DNS Slow Drip 攻撃」、「ランダムサブドメイン攻撃」、「ランダム DNS クエリー攻撃」、「NXDOMAIN 攻撃」といった呼称が使用されることもあります。

[ii] 「日本国内のオープン・リゾルバを踏み台とした DDoS 攻撃発生に起因すると考えられるパケットの増加について」（平成 26 年7月 23 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140723.pdf

[iii] 平成 26 年中の観測状況については、「情報技術解析平成 26 年報」の「6.3 オープン・リゾルバを悪用する新たな DDoS 攻撃手法に関する観測状況」も参照してください。
http://www.npa.go.jp/cyberpolice/detect/pdf/H26_nenpo.pdf

Copyright 2015 Cyber Force Center, NPA JAPAN

多発する可能性も十分に考えられます。同攻撃手法については、攻撃の対象となる権威DNSサーバにおいて実施可能な、かつ決定打となりうる有効な対策は現時点で存在しませんが、企業や組織等の管理者は攻撃の発生に備えて、以下の点に日頃から注意しておくことを推奨します。

- 日頃から権威 DNS サーバの稼働状況を把握し、攻撃発生を迅速に把握できる体制を構築しておくことを推奨します。
- 他の事業者が提供し、複数の顧客が共用する DNS サービスを利用している場合、自身が管理するドメインが攻撃対象とはならなくても、同一サービスを利用する他のドメインが攻撃被害を受けた場合には、その影響を受ける可能性があることに留意しておく必要があります。
- 攻撃を受けた場合には、処理能力に余裕がある外部 DNS サービスへの退避といった代替措置をとる対策も考えられます。このため、攻撃により正常な運用が妨害された場合の代替措置の必要性や具体的な手順について、平常時から検討を実施しておくことを推奨します。

2 MongoDB データベースに対する探索行為が増加[i]

MongoDB は、米国 MongoDB 社によって開発され、オープンソースで公開されているデータベースソフトウェアです。2月 10 日、ドイツのザールランド大学のグループは、インターネット経由で外部から認証を必要とせずにアクセスすることができる MongoDB データベースを約4万件確認したとの研究結果を公表しました。

MongoDB は初期設定では 27017/TCP ポートを使用します。2月 13 日以降、同ポートに対するアクセスの発信元 IP アドレス数が大きく増加しました（図2）。

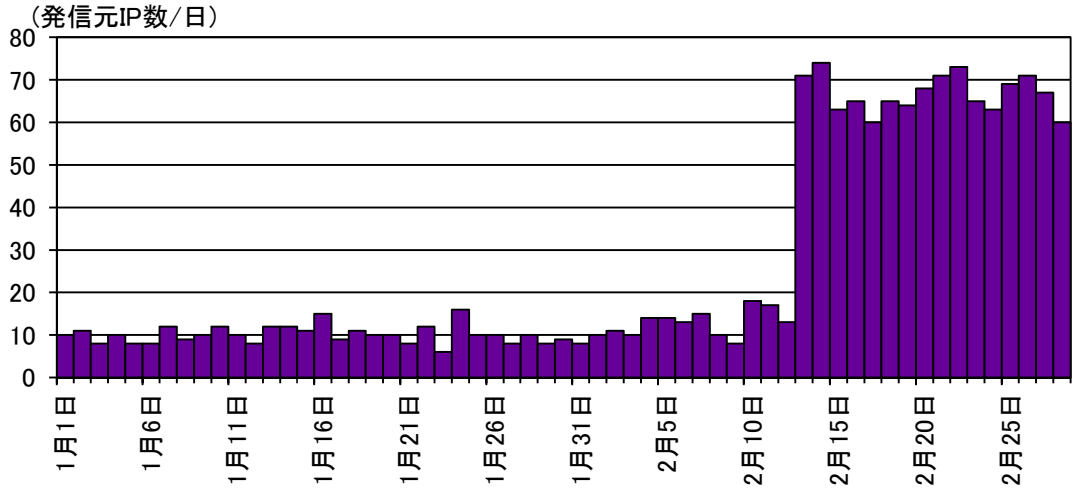

図2 宛先ポート 27017/TCP に対するアクセスの発信元 IP アドレス数の推移（H27.1.1～2.28）

[i] 本件については、以下の注意喚起を実施しています。
「MongoDB に対する探索行為の増加について」（平成 27 年2月 20 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20150220.pdf

Copyright 2015 Cyber Force Center, NPA JAPAN

また、アクセス内容を分析すると、単なるポートスキャン行為だけではなく、実際に MongoDB データベースの情報収集を試みる問い合わせを継続して多数観測しています（図3）。

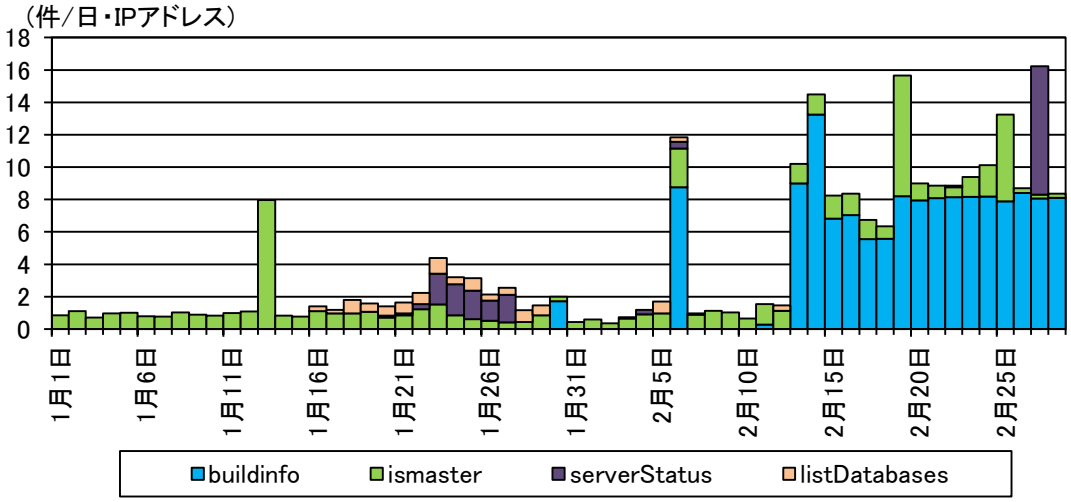

図3　MongoDB に対する問い合わせ内容別アクセス件数の推移（H27.1.1～2.28）

さらに、MongoDB データベースの情報収集を試みる問い合わせを行っている発信元 IP アドレスについて調査を実施したところ、その多くは、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（以下「非営利組織A」という。）や、あらゆるサービスに対して探索を実施して結果を蓄積するとともに、同結果の検索サービスを提供するサイト（以下「検索サイトB」という。）が管理すると考えられる IP アドレスからのアクセスでした。また、ザールランド大学が管理する IP アドレスからのアクセスも確認できました。しかしながら、クラウドコンピューティングサービス等を利用してアクセスを試みており、その背景や目的が判明しないアクセスも観測しています（図4）。このことから、データの窃取等を目的としてアクセスを実施している者が存在する可能性も十分に考えられるため、注意が必要です。

Copyright 2015 Cyber Force Center, NPA JAPAN

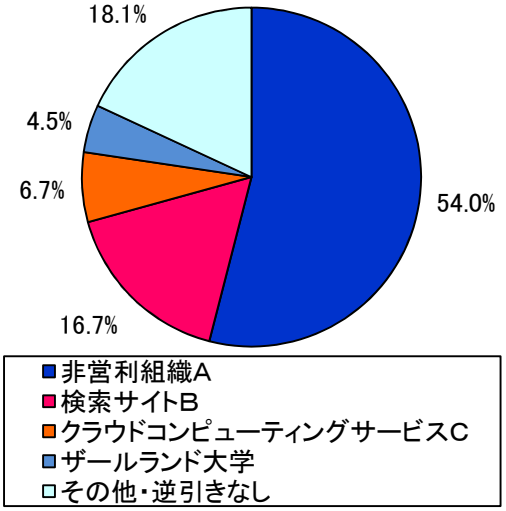

図4　発信元 IP アドレスの DNS 逆引き結果別の MongoDB 問い合わせ件数割合（H27.1.1～2.28）

Copyright 2015 Cyber Force Center, NPA JAPAN