JPCERT/CC

Japan Computer Emergency
Response Team Coordination Center

JPCERT-IA-2015-02
発行日 : 2015-04-27

JPCERT/CC インターネット定点観測レポート
[2015 年 1 月 1 日～3 月 31 日]

1　概況

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウエアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。なお、本レポートでは、本四半期に観測された日本宛のパケットを中心に分析した結果について述べます。

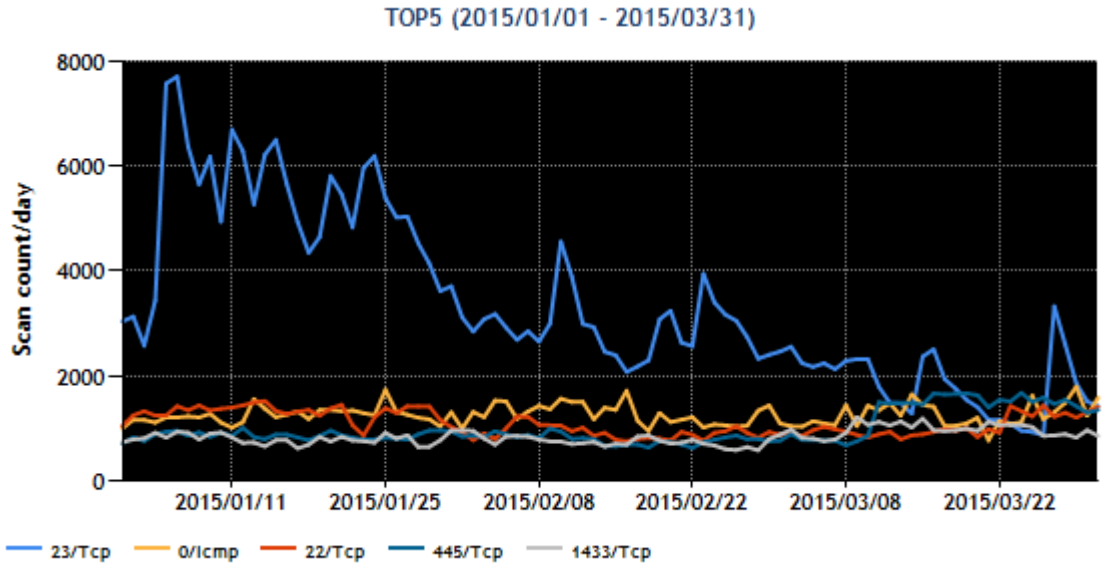
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[表 1 : 宛先ポート番号トップ 5]

順位	宛先ポート番号	前四半期の順位
1	23/TCP (telnet)	1
2	0/ICMP	4
3	22/TCP (ssh)	2
4	445/TCP (microsoft-ds)	3
5	1433/TCP (ms-sql-s)	5

※ポート番号とサービスの対応の詳細は、IANA の文書(*1)を参照してください。なお、サービス名は IANA の情報をもとに記載していますが、必ずしも各サービスプロトコルに則ったパケットが受信されているとは限りません。

図 1 は、期間中のトップ 5 の宛先ポート番号ごとのパケット観測数の推移を示しています。



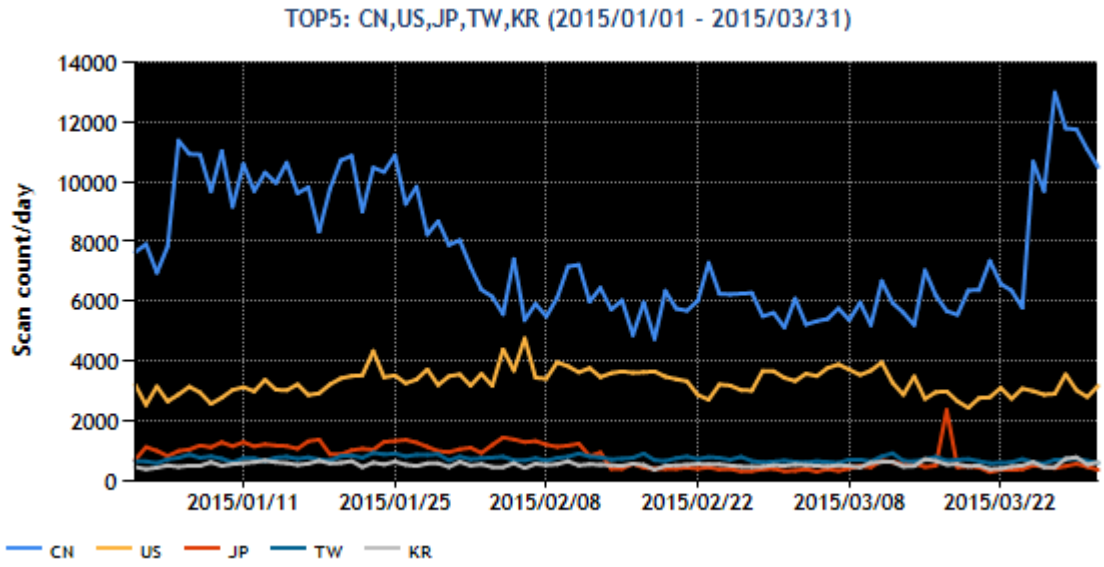
[図 1：2015 年 1~3 月の宛先ポート番号別パケット観測数トップ 5]

送信元地域のトップ 5 を [表 2]に示します。

[表 2：送信元地域トップ 5]

順位	送信元地域	前四半期の順位
1	中国	1
2	米国	2
3	日本	3
4	台湾	5
5	韓国	6

図 2 に期間中のトップ 5 のパケット送信元地域からのパケット観測数の推移を示します。



[図 2：2015 年 1~3 月の送信元地域別トップ 5 ごとのパケット観測数]

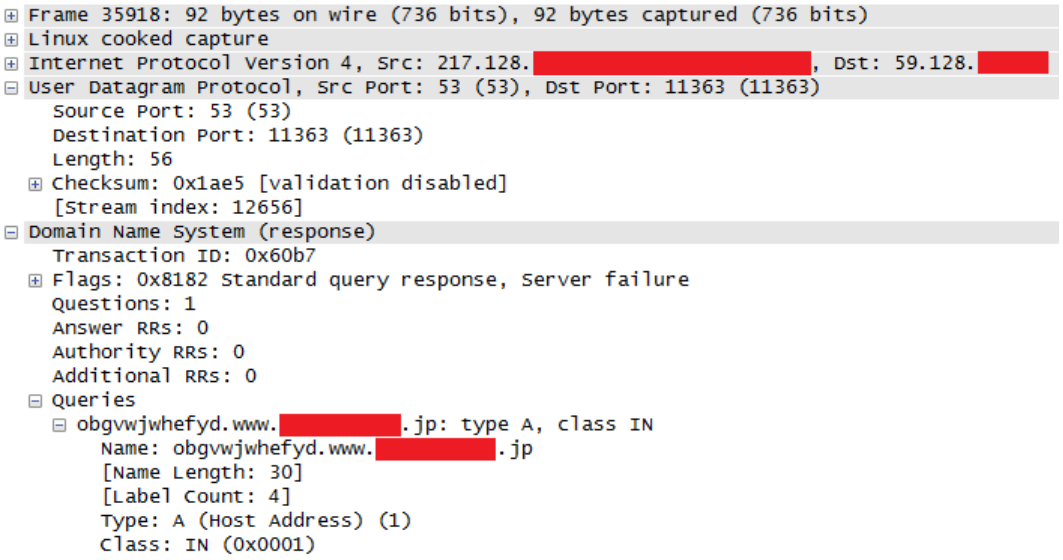
本四半期は、23/TCP 宛のパケットが 1 月以降減少しました。23/TCP の現象については、「2.2」で詳しく述べます。また、3 月中旬から 445/TCP 宛のパケットが増加しています。この増加の原因は、はっきりしませんが、新たな Conficker の亜種の活動も懸念されますので、Windows OS や Windows Server を使用している場合は、適切なセキュリティ対策(セキュリティ更新プログラムの適用や、ログオン認証に安易なパスワードを使用しないなど)の実施をお勧めします。その他については、多少の増減はありましたが、特筆すべき状況の変化は見られませんでした。

2　注目された現象

2.1　国内の機器を含むオープンリゾルバが使用された DDoS 攻撃の観測

過去の定点観測レポート [*2] で、国外のドメインが対象となった DDoS 攻撃において、オープンリゾルバを使用し、存在しない多数の FQDN を問い合わせることによって攻撃対象の権威 DNS サーバに過剰な負荷を加えようとする攻撃(以下「DNS 水責め攻撃」といいます。)の手法が使用された事例を紹介しましたが、2 月上旬にトップレベルドメインが「JP」である国内のドメイン(以下「国内ドメイン」といいます。)を攻撃対象とした、送信元ポート番号が 53/UDP のパケット(以下「DNS 応答パケット」といいます。)および DNS サービスのポート不達を示す ICMP エラーパケット(Destination unreachable)を多数観測しました(図 3 を参照)[*3]。

トップレベルドメインが JP であるドメインを対象とする DDoS 攻撃で、DNS 水責め攻撃の手法が使用された初の事例だと JPCERT/CC は考えています。



[図 3：2015 年 2 月の送信元ポート番号 53/UDP のパケット(Wireshark による表示)]

今回の DNS 水責め攻撃の対象となった国内ドメインは、国内のドメイン登録代行事業者が運用する権威 DNS サーバに登録されていました。この権威 DNS サーバは、国内でも利用者数の多い複数のサイトのドメインを管理していました(以下、複数ドメインを管理する権威 DNS サーバを「共有 DNS サーバ」という。)。このため攻撃により国内の共有 DNS サーバに過剰な負荷が上がることで、対象となった国内ドメインだけではなく、同一の共有 DNS サーバで管理されていた複数のドメイン(クラウドを使用したサービスを提供している事業者やオンラインゲームなど)も名前の解決ができなくなり、Web サイトが閲覧できない、メールが受け取れないなどの問題が発生していたと推測されます。

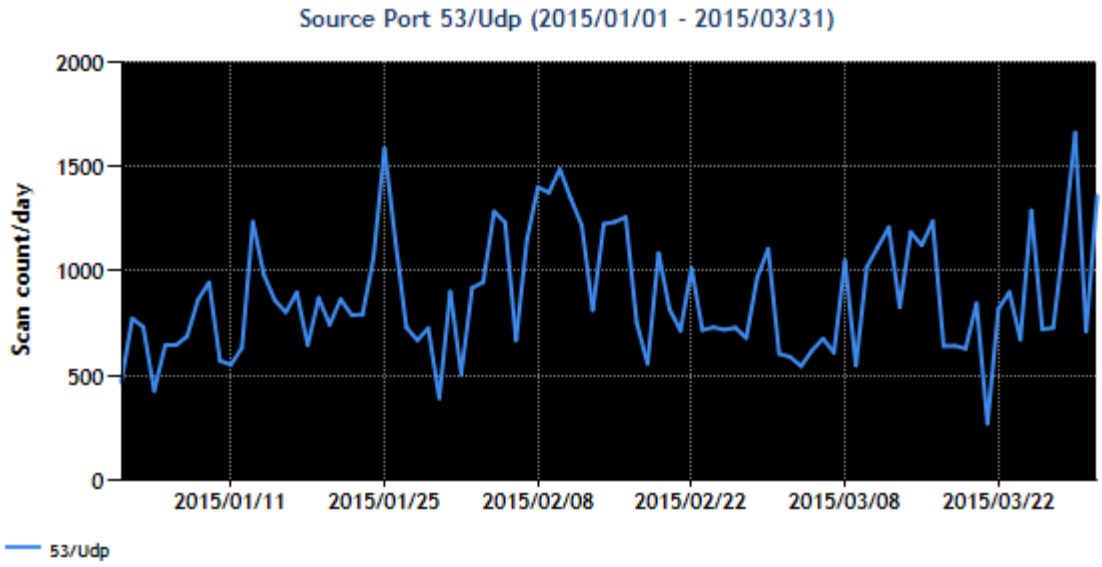
さらに、この国内の共有 DNS サーバが応答しない状態に陥ったことで、攻撃に加担したオープンリゾルバも、国内の共有 DNS サーバ間にある複数の ISP などのキャッシュ DNS サーバも、共有 DNS サーバからの応答を待つ問合せ処理が多数積み上がり、異常に負荷が上がります。これによりキャッシュ DNS サーバの利用者にも同様に Web サイトの閲覧ができない、メールの送受信ができないなどの問題が発生していたと推測されます。

なお、WHOIS 情報を確認したところ、国内ドメインは、攻撃発生当初は、国内の共有 DNS サーバに登録されていましたが、その後、海外の事業者が運用する共有 DNS サーバに変更されていました。これは、本攻撃への対策として行われた変更と推測されます。

3 月上旬には、米国の大手レジストラが運用する共有 DNS サーバで管理されていたドメインが対象となる DNS 応答パケットおよび DNS サービスのポート不達を示す ICMP エラーパケットを観測しました。この米国のレジストラの共有 DNS サーバは、国内サイトのドメインの登録先としても利用されるケースがあり、この共有 DNS サーバを利用していたドメインは、本攻撃により、Web サイトが閲覧できないなどの障害が発生していた可能性があります。

図 4 は、本四半期の送信元ポート番号が 53/UDP とするパケット観測数のグラフです。グラフのパケッ

ト全てが DDoS 攻撃パケットではありませんが、DDoS 攻撃を目的としたと思われるパケットを多く観測しています。



[図 4：2015 年 1 月から 3 月の送信元ポート番号 53/UDP のパケット観測数]

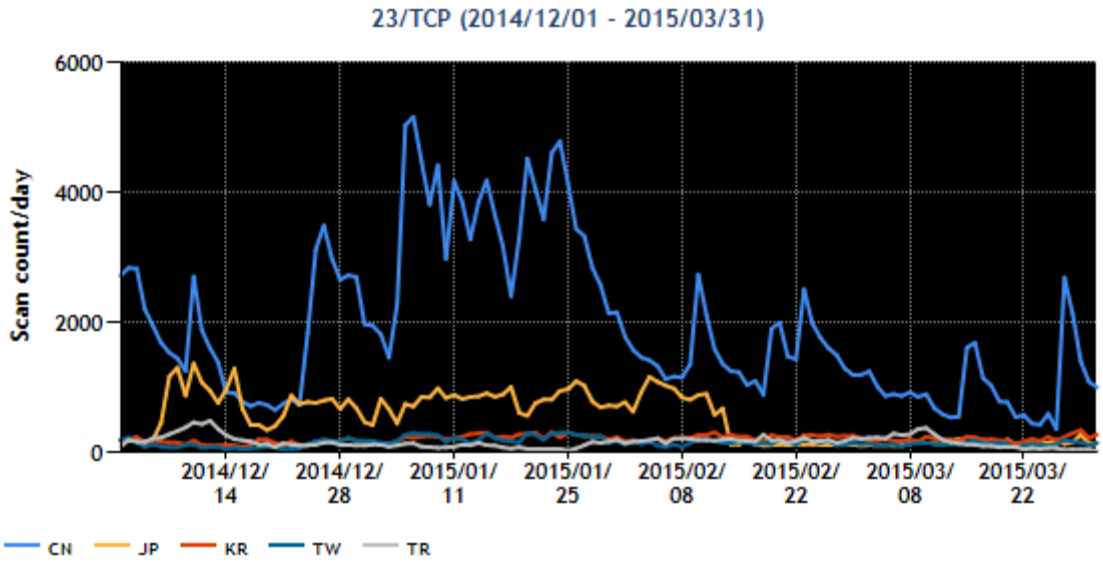
今回 JPCERT/CC で確認した国内ドメインを対象とする DNS 水責め攻撃だけでなく、日頃から発生している海外のドメインを対象とする DNS 水責め攻撃や DNS Amp 攻撃などに関連しても多数のオープンリゾルバが国内に存在しており、意図的ではないにせよ DDoS 攻撃に加担する結果となっていることは我が国として由々しき問題です。攻撃の踏み台となっているオープンリゾルバを減らすために、特に次の点について確認してください。

1. DNS サーバを運用している場合は、再帰的な問合せを受け付ける範囲など、設定を再確認し、必要最小限になるようアクセス制限を施してください。(* 4,5,6)
2. インターネット接続用ルータなどで DNS サーバや DNS フォワーダ機能を持つネットワーク機器を使用している場合は、不特定のホストからの DNS 問合せに応答しない設定になっていることを確認してください。各製品ベンダから公開されている情報を参考に、設定の確認をお勧めします。(*6,7)
3. Web サーバなどの公開サーバを運用している場合は、管理するサーバで不要な DNS サーバが稼働していないか念のため確認してください。

なお、JPCERT/CC では、オープンリゾルバを減らすための活動の一環として、インターネット定点観測システムで観測した DNS 応答パケットおよび DNS サービスのポート不達を示す ICMP エラーパケットを調査し、その送信元となっている国内の IP アドレスの管理者に対して調査を依頼しています。

2.2　23/TCP 宛のパケットの減少

図 5 が示すように、本四半期は、23/TCP 宛のパケットが 1 月以降減少しました。23/TCP 宛のパケットの送信元地域は、中国が約 54%を占めていますが、1 月以降、中国を送信元とするパケットが大きく減少したのに伴い総数でも減少傾向となりました。中国からのパケットの減少の原因は不明です。送信元地域が国内のパケットも本四半期の 2 月上旬から減少しています。前四半期から観測した国内を送信元とする 23/TCP 宛のパケットの増加は、過去の定点観測レポートの「2.1 23/TCP, 8080/TCP 宛へのパケットの増加」(*8)で紹介しましたが、これは、既知の脆弱性(いわゆる Shellshock)をもつ QNAP 社製の Network Attached Storage(NAS)製品(以下 QNAP NAS」といいます。)のマルウエア感染に起因すると思われるものでした。



[図 5：2014 年 12 月～2015 年 3 月の 23/TCP 宛のパケット観測数(送信元地域別)]

JPCERT/CC では、攻撃の踏み台となっているマルウエア感染を減らすため、観測した 23/TCP 宛のパケットの送信元ノードを網羅的に調査し、国内にあり QNAP NAS の稼働を確認できた場合に、IP アドレスの管理者などに対して調査を依頼しました（動的 IP アドレスが割り当てられているノードについては重複して連絡した可能性があります)。調査を依頼した管理者などからは、「対策を実施する」「NAS に不審なユーザが作成されていることを確認したので対応した」「当該機器を撤去した」などの返答をいただきました。

図 5 が示すように、国内を送信元とする 23/TCP 宛のパケット数は 2 月上旬以降に減少しました。この理由は、マルウエアの挙動の変化とのた可能性も完全には否定はできませんが、JPCERT/CC からの要請に応じた QNAP NAS の利用者によるマルウエア駆除と対策が進んだ結果と考えています。

3 参考文献

(1) Service Name and Transport Protocol Port Number Registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
(2) JPCERT/CC インターネット定点観測レポート(2014 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201404-06.html
(3) 警察庁@Police
インターネット観測結果等 (平成 27 年 2 月期)
https://www.npa.go.jp/cyberpolice/detect/pdf/20150331.pdf
(4) 株式会社日本レジストリサービス(JPRS)
DNS サーバの不適切な設定「オープンリゾルバー」について
http://jprs.jp/important/2013/130418.html
(5) 日本ネットワークインフォメーションセンター
オープンリゾルバ(Open Resolver)に対する注意喚起
https://www.nic.ad.jp/ja/dns/openresolver/
(6) JPCERT/CC
オープンリゾルバ確認サイト
http://www.openresolver.jp/
(7) JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
https://jvn.jp/jp/JVN62507275/
(8) JPCERT/CC インターネット定点観測レポート(2014 年 10～12 月)
https://www.jpcert.or.jp/tsubame/report/report201410-12.html#2.1

本活動は、経済産業省より委託を受け、「平成２６年度サイバー攻撃等国際連携対応調整事業」として実施したものです。