JPCERT/CC®

JPCERT-IA-2015-04
発行日 : 2015-10-29

JPCERT/CC インターネット定点観測レポート
[2015 年 7 月 1 日～9 月 30 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。

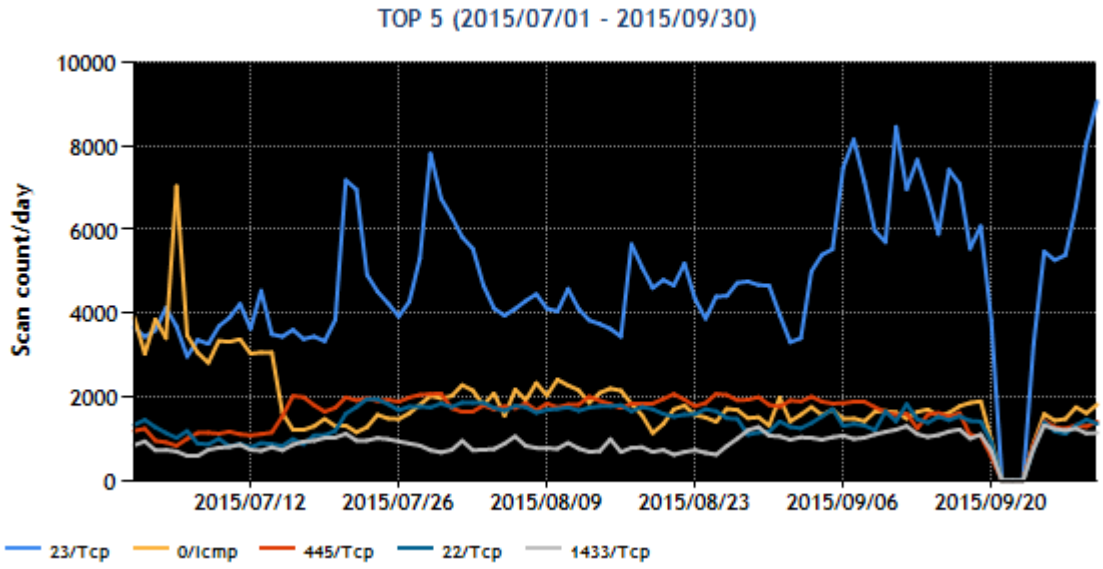
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[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	445/TCP (microsoft-ds)	2
4	22/TCP (ssh)	5
5	1433/TCP (ms-sql-s)	6

※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。なお、2015 年 9 月 20 日 14 時 50 分から 9 月 24 日 9 時 20 分にかけて、インターネット定点観測システムの収容施設の設備に問題が発生し、システムの運用を停止したため、この期間の観測データが欠落しています。



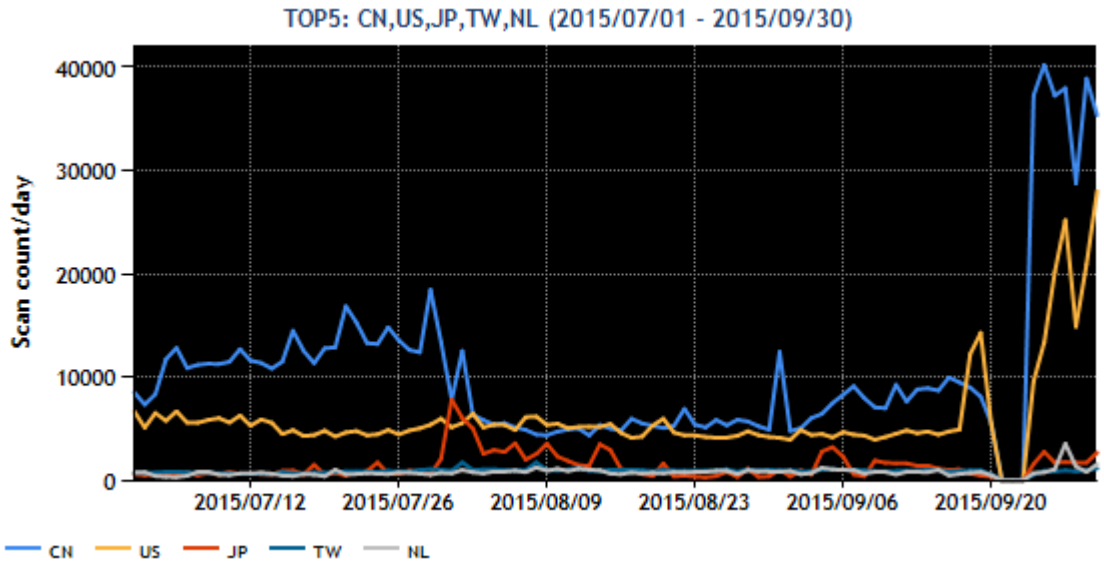
[図 1：2015 年 7~9 月の宛先ポート番号別パケット観測数トップ 5]

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	4
4	台湾	3
5	オランダ	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。



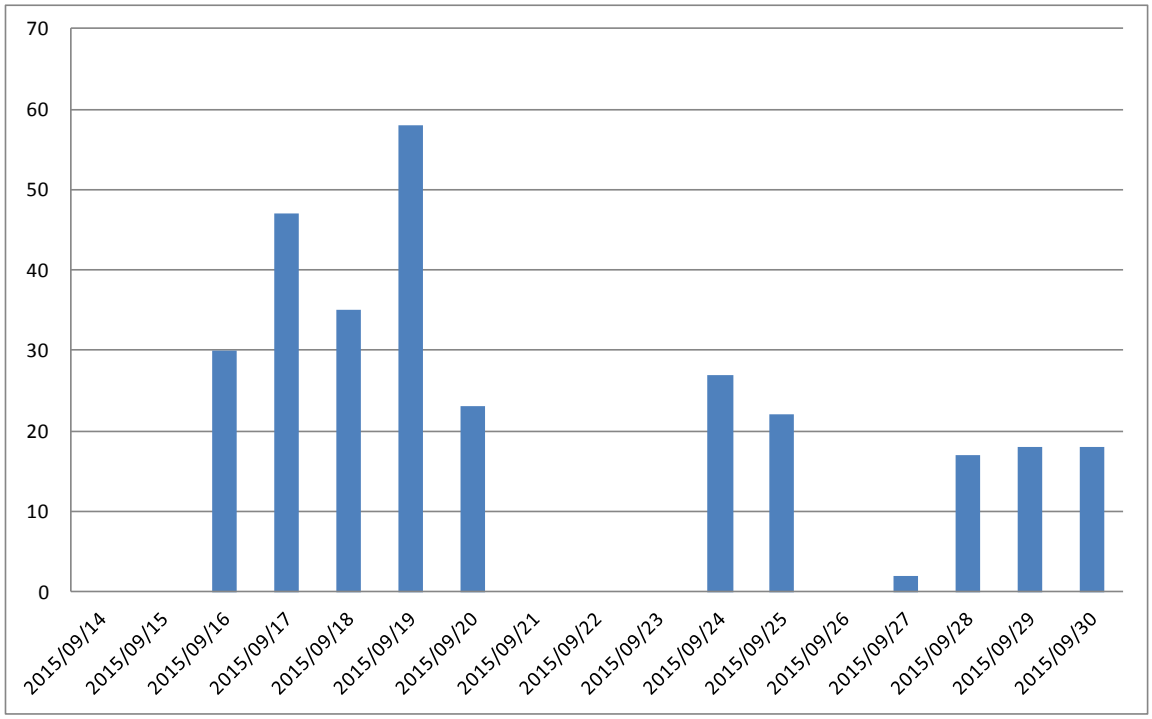
[図 2：2015 年 7~9 月の送信元地域別トップ 5 ごとのパケット観測数]

Telnet サーバを搭載したネットワーク機器を探索する活動については、過去の定点観測レポートでも紹介しましたが、本四半期も 23/TCP 宛のパケットを多数観測しています。また、9 月 24 日から 10 月上旬に、主に中国、米国を送信元とするパケット数が増加しました。しかしながら、これは特定のセンサーが 1900/UDP 宛に SSDP の M-SEARCH リクエストのパケットを一時的に多数受信した影響によるものです。このセンサー以外では、顕著な変化が見られなかったことから、広域的な脅威を示すデータではないと判断しています。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　SYNful Knock が設置された Cisco 社製ルータを探索するパケット

9 月中旬よりマルウエア SYNful Knock が設置された Cisco 社製ルータを探索する目的と推測される 80/TCP 宛のパケットを継続して観測しています。2015 年 9 月中旬以降について、その観測数を図 3 に示します。



[図 3. SYNful Knock が設置された Cisco 社製ルータの探索と推測されるパケットの観測数]

Cisco 社は、8 月 11 日に Cisco IOS Software Platform を狙う攻撃についての注意喚起(*2)を公開しました。この情報によると、同社製ルータが何らかの方法で侵入され、マルウエア (細工された ROMMON image) が設置される事例が確認されています。その後、セキュリティベンダである FireEye 社が 9 月 15 日に、Cisco 社製ルータに設置されるマルウエアを SYNful Knock と称し、このマルウエアの調査結果 (挙動や感染しているかどうかの探索方法など) を公開(*3)しました。Cisco 社は、FireEye 社の記事を受けて、改めて注意を促す記事(*4)を公開しています。

FireEye 社が公開した探索方法は、攻撃者が SYNful Knock が設置された Cisco 社製ルータをコントロールするパケットの特徴を使用したもので、このパケットに応答する内容によって SYNful Knock が設置されているかどうかを判断しています。9 月中旬からインターネット定点観測システムで観測しているパケット (図 3) は、FireEye 社が公開した探索方法に現れるパケットと同じものであることから、これらは SYNful Knock が設置されている Cisco 社製のルータを探索する目的と推測しています。

なお、SYNful Knock の設置状況を調査したミシガン大学やカリフォルニア大学などのグループ(*5)による

と、9 月中旬時点では、SYNful Knock が設置された Cisco 社製ルータがインド、メキシコ、フィリピン、ウクライナでは確認されていますが、日本国内では見つかっていません。

これらの状況からわかるように、インターネットからアクセスできるノードは、攻撃対象となりえます。万が一、ルータが侵入されると、内部ネットワークへの侵入や、マルウエア感染、情報詐取など様々なリスクが考えられます。適切なセキュリティ対策 (デフォルトパスワードを使用しない、脆弱性を修正したファームウェアに更新、セキュリティ設定の再確認など) を実施して、攻撃の踏み台に使用されないよう努めてください。

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) Evolution in Attacks Against Cisco IOS Software Platforms
http://tools.cisco.com/security/center/viewAlert.x?alertId=40411

(3) SYNful Knock - A Cisco router implant - Part I
https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

(4) SYNful Knock: Detecting and Mitigating Cisco IOS Software Attacks
http://blogs.cisco.com/security/synful-knock

(5) In Search of SYNful Routers
https://zmap.io/synful/

本活動は、経済産業省より委託を受け、「平成２７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。