JPCERT-IA-2014-02
発行日 : 2014-04-21

JPCERT/CC インターネット定点観測レポート
[2014 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います。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、2014 年 1 月 1 日から 3 月 31 日の期間（以下、本四半期と記す）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。

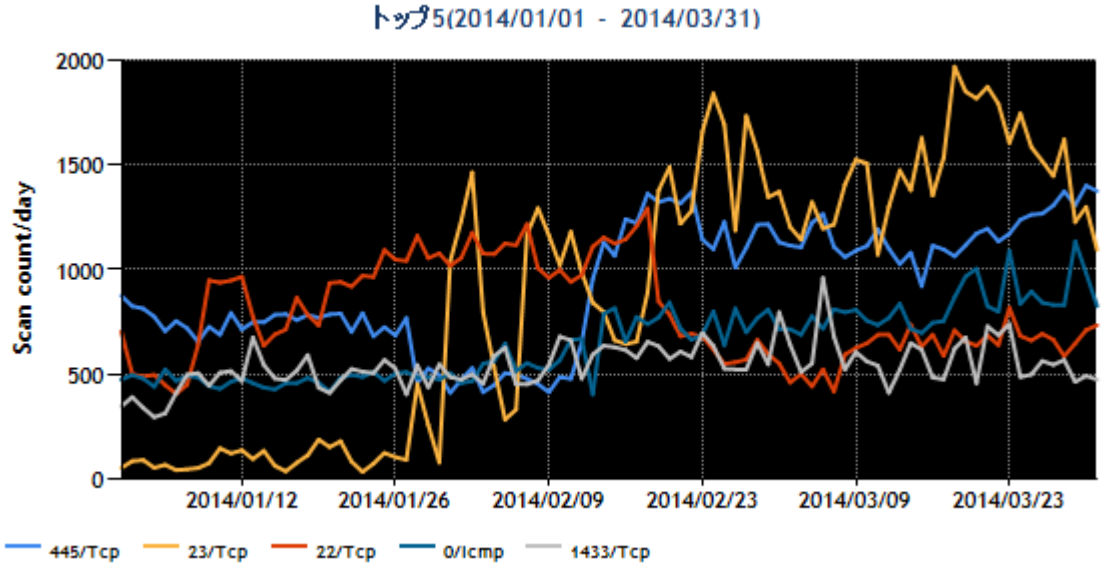
本四半期に観測した宛先ポート番号別パケット観測数のトップ 5 を[表 1]に示します。

[表 1 : 宛先ポート番号トップ 5]

2013 年 10～12 月		2014 年 1～3 月	
1	445/TCP (microsoft-ds)	1	445/TCP (microsoft-ds)
2	0/ICMP	2	23/TCP (telnet)
3	1433/TCP (ms-sql-s)	3	22/TCP (ssh)
4	22/TCP (ssh)	4	0/ICMP
5	3389/TCP (ms-wbt-server)	5	1433/TCP (ms-sql-s)

※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時間的な変化を示しています。



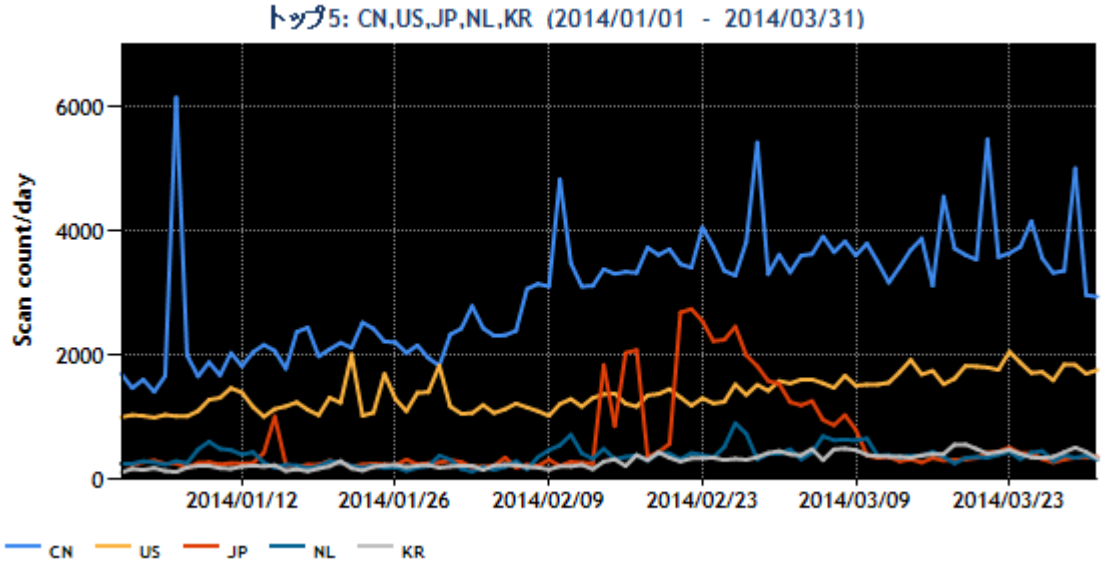
[図 1　2014 年 1~3 月の宛先ポート番号別パケット観測数トップ 5]

本四半期に観測した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]

2013 年 10～12 月		2014 年 1～3 月	
1	中国	1	中国
2	米国	2	米国
3	オランダ	3	日本
4	日本	4	オランダ
5	ロシア	5	韓国

図 2 に期間中のパケット送信元地域トップ 5 の変化を示します。



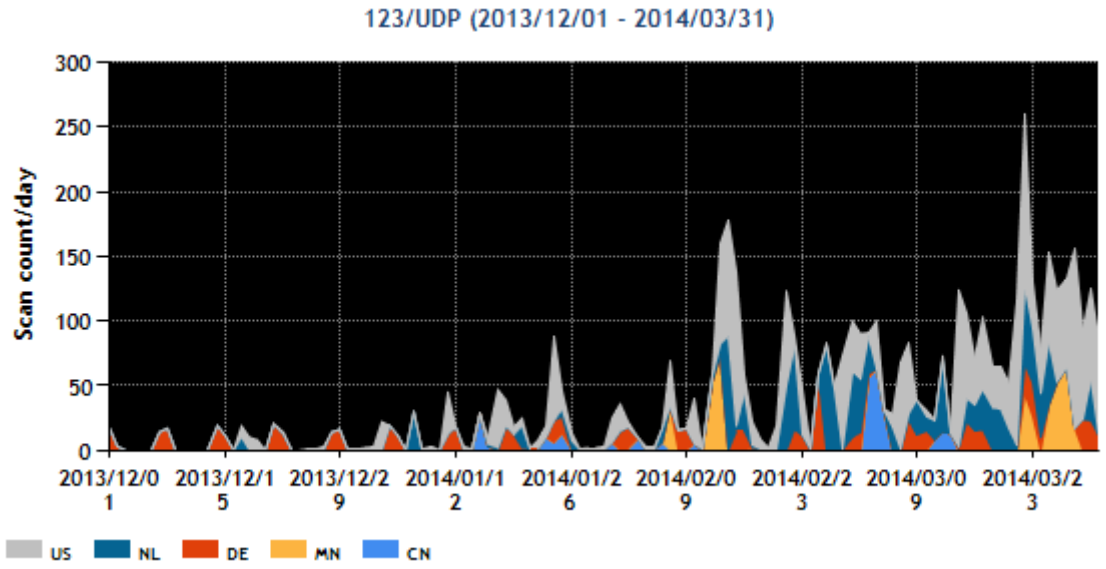
[図 2　2014 年 1~3 月の送信元地域別トップ 5]

1 月下旬以降において 445/TCP、23/TCP 宛のパケット数が増加しました。本四半期パケット観測数が 2 位となった 23/TCP の現象については、「2.1」で詳しく述べます。2 月中旬に、送信元地域を日本とするパケット数の増加が見られます。これは、特定のセンサーが 13832/TCP、43962/TCP、12591/TCP 宛のパケットを多数受信した影響です。JPCERT /CC では、これらのポートを使用する製品や脆弱性などの情報を調査しましたが、該当する情報が無く、また、特定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すが、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

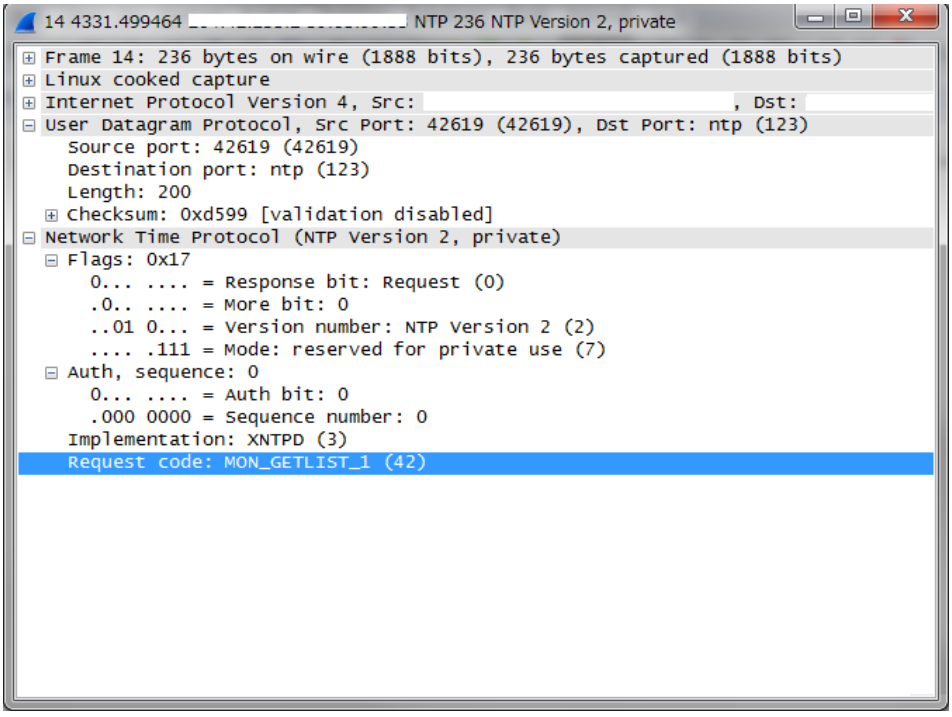
2.1　123/UDP ポート宛へのパケットの増加

前号の定点観測レポート[*2]で報告した 123/UDP (NTP) 宛のパケットの増加が本四半期も続いています。特に米国およびオランダを送信元とするパケット数の増加が目立ちました。



[図 3 2013 年 12～3 月の 123/UDP 宛のパケット観測数]

CloudFlare 社の情報 (*3,4)によると、2014 年 2 月にヨーロッパにおいて NTP サーバが使用された DDoS 攻撃（約 400Gbps に達する）が発生しています。また、国内に設置した観測用センサーにおいても、NTP サーバの状態を問い合わせる機能 (monlist) を使う探索と思われるパケットを定期的に受信しています (図 4 は、国内のセンサーで受け取ったパケットの一つです)。



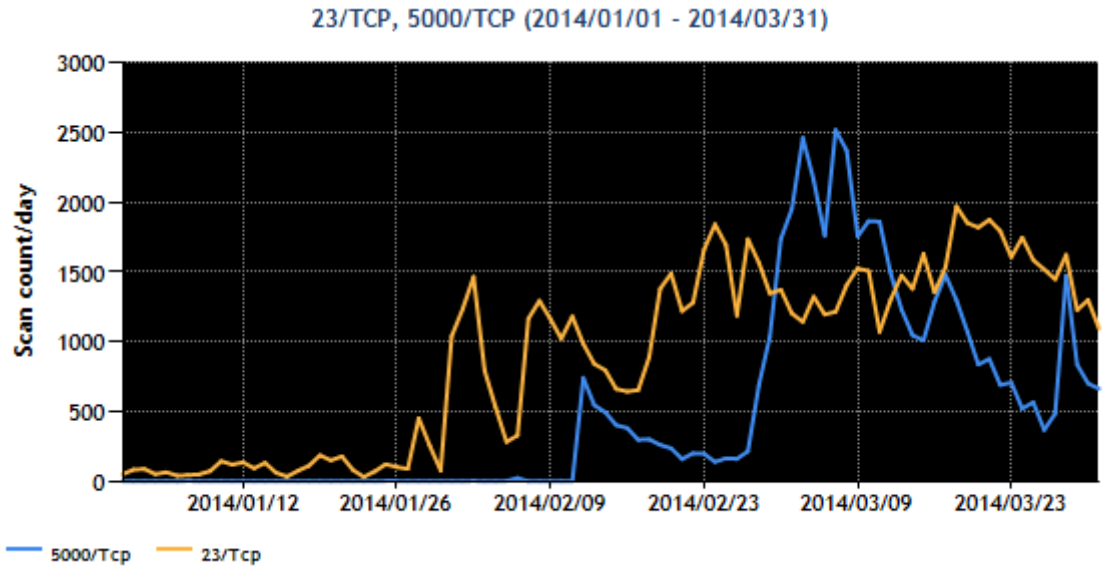
[図 4 2014 年 1 月の 123/UDP 宛のパケット(Wireshark による表示)]

今後も、NTP サーバを探索する活動や、NTP サーバを使用した DDoS 攻撃が行われる可能性がありますので、管理下のサーバやネットワーク機器などで NTP サーバの稼働状況を確認し、攻撃に使用されないよう適切なセキュリティ対策 (パッチやアップデート、アクセス制御、セキュリティ設定の再確認など)[(*5,6,7)]を実施してください。

2.2 23/TCP、5000/TCP 宛へのパケットの増加

本四半期は、1 月下旬から、23/TCP 宛へのパケット数が増加しました。telnet を待ち受けるサーバを搭載したネットワーク機器を対象とする探索活動が再び発生しています (過去の定点観測レポート[8,9]でも telnet サーバの探索活動を紹介しました)。

本四半期の特徴は、23/TCP 宛のパケット数の増加と時期を同じくして 2 月上旬から 5000/TCP 宛のパケット数が増加し、本四半期の宛先ポート番号別パケット観測数の 6 位となっています。これは、マルウエアに感染したネットワーク機器が、宛先をポートを 23/TCP だけでなく脆弱性が存在する NAS[(*10)]が使用する 5000/TCP も探索[(*10)]していたものと推測されます。



[図 5 23/TCP、5000/TCP 宛のパケット観測数]

本四半期に観測した 23/TCP、5000/TCP 宛のパケットの送信元地域のトップは共に中国で、パケット数の全体のうち 23/TCP 宛のパケットでは約 6 割、5000/TCP 宛のパケットでは、約 3 割を中国が占めました。JPCERT/CC では、23/TCP、5000/TCP 宛へのパケットを送信する IP アドレスについて調査したところ、その多くで外国製の特定のネットワークカメラ製品が稼働していました。国内の IP アドレスからの探索活動を観測しており、当該製品が設置されていたことを確認しました。

インターネット上に設置されたネットワークカメラや NAS などのネットワーク機器も探索の対象[*11,12,13] となっていますので、これらの機器においても適切なセキュリティ対策 (パッチやアップデート、アクセス制御、セキュリティ設定の再確認など) を実施してください。

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) JPCERT/CC インターネット定点観測レポート (2013 年 10～12 月)
https://www.jpcert.or.jp/tsubame/report/report201301-03.html

(3) Technical Details Behind a 400Gbps NTP Amplification DDoS Attack
http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

(4) Understanding and mitigating NTP-based DDoS attacks
http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks

(5) Japan Vulnerability Notes JVNVU#96176042
NTP が DDoS 攻撃の踏み台として使用される問題
https://jvn.jp/cert/JVNVU96176042/index.html

(6) Vulnerability Note VU#348126
NTP can be abused to amplify denial-of-service attack traffic
http://www.kb.cert.org/vuls/id/348126

(7) ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140001.html

(8) JPCERT/CC インターネット定点観測レポート(2012 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201201-03.html

(9) JPCERT/CC インターネット定点観測レポート(2012 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201204-06.html

(10) Japan Vulnerability Notes JVNVU#95919136
Synology DiskStation Manager にアクセス制御不備の脆弱性
https://jvn.jp/vu/JVNVU95919136/

(11) 脆弱性が存在する NAS の探索と考えられる宛先ポート
5000/TCP に対するアクセスの急増について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf

(12) More Device Malware: This is why your DVR attacked my Synology DiskStation (and now with Bitcoin Miner!)
https://isc.sans.edu/forums/diary/More+Device+Malware+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+and+now+with+Bitcoin+Miner/17879

(13) IoT ワームを利用した暗号通貨のマイニング
http://www.symantec.com/connect/blogs/iot

本活動は、経済産業省より委託を受け、「平成 25 年度情報セキュリティ対策推進事業」として実施したものです。