平成 26 年 5 月 21 日

インターネット観測結果等
(平成 26 年 4 月期)

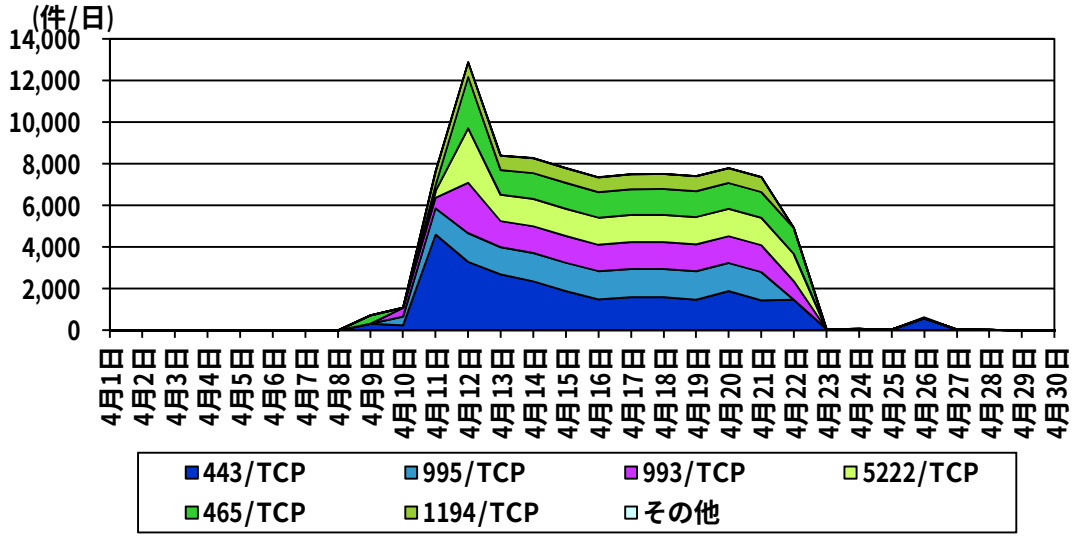
- OpenSSL の脆弱性を標的としたアクセスの検知
- ビル管理システムに対する探索行為の検知
- 53/UDP を発信元としたパケットの更なる増加

1 OpenSSL の脆弱性を標的としたアクセスの検知

警察庁の定点観測システムにおいて、平成 26 年 4 月 9 日以降、当該攻撃コードに実装されている Client Hello パケット[1]と完全に一致するパケットを観測しており、10 日に注意喚起を実施しました[2]。その後もパケットは増加し、ピーク時の 12 日には 12,881 件/日のパケットを観測しました。その後、22 日まで 8,000 件/日程度のパケットを継続して観測しました（図1）。

宛先ポートは、443/TCP、995/TCP、993/TCP、5222/TCP、465/TCP 及び 1194/TCP を観測しており（表1）、HTTPS に使用される 443/TCP ポート以外にも OpenSSL が使用されているサービスを満遍なく検索している状況が伺われます。

23 日以降観測されるパケットは、急激に減少していますが、継続して観測されていることからから今後も、注意する必要があります。



[1] SSL/TLS 通信において、TCP3ウェイハンドシェイク確立後、クライアントからサーバに対して送信される最初のパケット。

[2] OpenSSL の脆弱性を標的としたアクセスの増加について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140410.pdf

図1　攻撃コードに実装されている Client Hello パケットの宛先ポート別検知件数の推移

表1　検知順位別のポート番号一覧

順位	ポート番号	概要
1	443/TCP	HTTPS (Hypertext Tranfer Protocol over TLS/SSL) に使用されるポートである。
2	995/TCP	POP3S(Post Office Protocol 3 over TLS/SSL)に使用されるポートである。
3	993/TCP	IMAPS(Internet Message Access Protocol over TLS/SSL)に使用されるポートである。
4	5222/TCP	XMPP(インスタントメッセンジャー)で使用されるポートである。
5	465/TCP	SMTP over SSL (メール転送) に使用されるポートである。
6	1194/TCP	OpenVPN で使用されるポートである。

2　ビル管理システムに対する探索行為の検知

3月中旬から検知していた、代表的なビル管理システムである「BACnet (Building Automation and Control Networking protocol)」の探索行為と考えられるアクセス (ポート番号 47808/UDP) を、4月にも継続して確認しています (図2)。

警察庁では、4月[1]及び5月[2]に注意喚起を実施しているので、対策等については、そちらを確認して下さい。

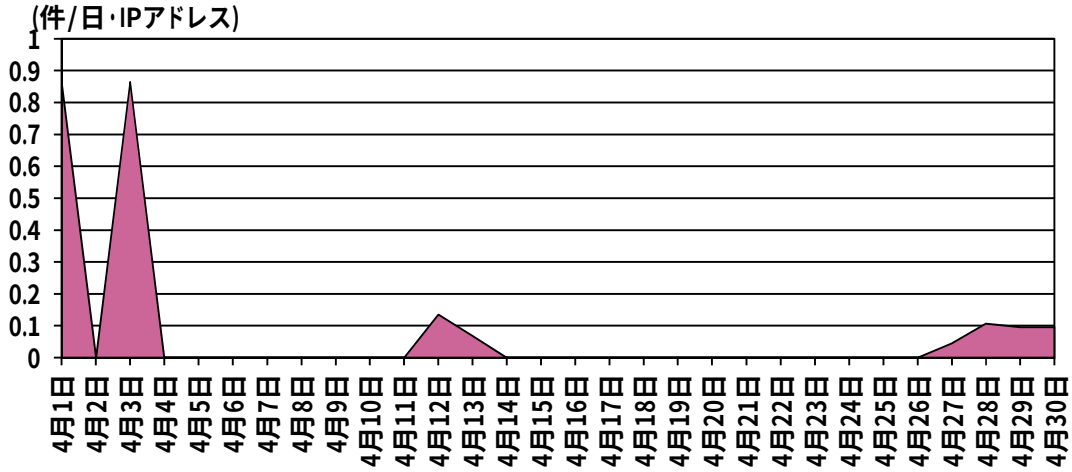


図2　BACnet の探索行為と考えられるアクセス件数の推移

[1] ビル管理システムに対する探索行為の検知について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140404.pdf

[2] ビル管理システムに対する探索行為の検知について (第2報)
http://www.npa.go.jp/cyberpolice/detect/pdf/20140508.pdf

3　53/UDP を発信元としたパケットの更なる増加

2月4日以降継続して観測していた 53/UDP を発信元とするパケットが、4月上旬にピークを迎えました（図3）。

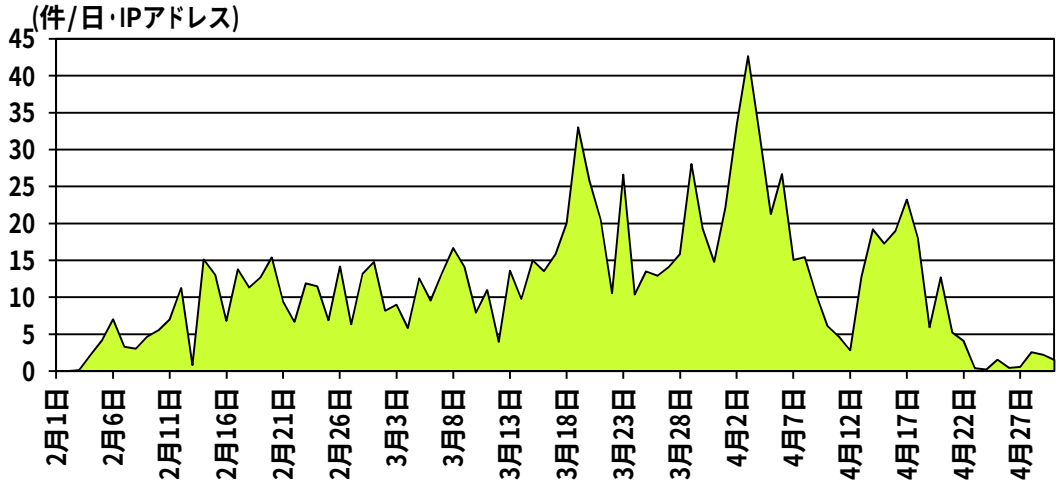


図3　53/UDP を発信元ポートとするアクセス件数の推移（2月1日～4月 30 日）

「発信元 IP アドレスを偽装したオープン・リゾルバの探索行為の増加について」[1]及び「インターネット定点観測（平成 26 年2月期）」[2]でも述べたとおり、このパケットは、DNS 問い合わせに対する応答パケットであり、何者かが発信元 IP アドレスを偽装した上で、当該 DNS サーバを踏み台とした DNS リフレクター攻撃の実行可否の調査を実施した可能性が考えられるものです。

4月下旬以降も、観測件数は減少しているものの、継続して観測しています。

[1] http://www.npa.go.jp/cyberpolice/detect/pdf/20140217.pdf
[2] http://www.npa.go.jp/cyberpolice/detect/pdf/20140328.pdf