平成 27 年 12 月 16 日

Topic

Slow HTTP DoS Attack に対する注意喚起について

警察庁では Slow HTTP DoS Attack の可能性が疑われる攻撃事例を把握しました。Web サーバの管理者は、同攻撃への対策を必要に応じて検討することを推奨します。

1 Slow HTTP DoS Attack について

Slow HTTP DoS Attack は、共通した特徴を持つ複数の DoS 攻撃手法の総称であり、Slow Client Attack 又は Slow Rate Attack とも呼称されます。これらの攻撃手法は以前から知られているものであり、決して新しい手法ではありません。しかしながら、警察庁では同手法が悪用された可能性がある攻撃事例を把握したことから、注意喚起を実施するものです。

ソフトウェアの脆弱性を悪用する手法を除けば、一般的な DoS 攻撃手法は、大量のパケットを攻撃対象に送信することにより、回線帯域やサーバ等の処理能力を逼迫させることを目的とするものです。しかしながら、Slow HTTP DoS Attack では、比較的少ないパケット数で長時間に渡り TCP セッションが継続するように操作することにより、Web サーバの TCP セッションを占有し、正規のサイト閲覧者がアクセスできないように妨害を行います。他の代表的な DoS 攻撃手法[i]との相違点は表1のとおりです。

表1 代表的な DoS 攻撃手法の相違点

代表的な DoS 攻撃手法	パケット数	攻撃手法の概要
UDP flood ICMP flood リフレクター攻撃(アンプ攻撃)	多	サイズが大きな UDP もしくは ICMP パケットを多数送信することにより、回線帯域を逼迫させる。
SYN flood Connection flood リロード攻撃(F5 攻撃)	多	多数の TCP パケットを送信することにより、サーバ等の TCP セッションを占有する。
Slow HTTP DoS Attack	少	各 TCP セッションの継続時間を可能な限り引き延ばすことにより、Web サーバ等の TCP セッションを占有する。

Slow HTTP DoS Attack では、サイズの小さな通信を Web サーバと繰り返し行うことにより、TCP セッションの継続時間を引き延ばします。同攻撃手法は、継続時間の引き延ばしを試みる通信の対象により、さらに次の3種類に分類されます。

(1) Slow HTTP Headers Attack

Slow HTTP Headers Attack は、待機時間を挟みながら、長大な HTTP リクエストヘッダを送信し続けることにより、TCP セッションの占有を図る攻撃手法です。同手法は平成 21

[i] その他の代表的な DoS 攻撃手法については、以下の資料を参照してください。
「Dos/DDoS 対策について」(平成 15 年 6 年 3 日)
http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf

年（2009 年）に「Slowloris」と命名された攻撃ツールが公開されたことにより、広く知られるようになりました。このため、Slowloris Attack と呼ばれることもあります。

(2) Slow HTTP POST Attack

Slow HTTP POST Attack は、HTTP の POST メソッドを悪用して、待機時間を挟みながら、長大な HTTP リクエストボディ（POST ペイロード）を送信し続けることにより、TCP セッションの占有を図る攻撃手法です。同手法は平成 22 年（2010 年）に2名の研究者[i]によって明らかにされました。代表的な攻撃ツールの名称から R.U.D.Y Attack と呼ばれることもあります。

(3) Slow Read DoS Attack

Slow Read DoS Attack は、非常に小さな TCP ウィンドウサイズを指定して、Web サーバからの HTTP レスポンスを少しずつ受信することにより、セッションの継続時間を引き延ばす攻撃手法です。同手法は平成 24 年（2012 年）にセキュリティ対策企業[ii]によって明らかにされました。

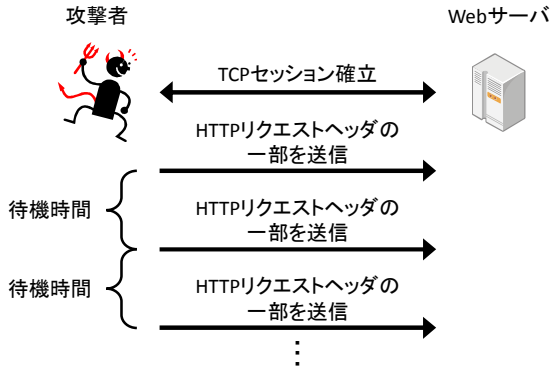

図1　Slow HTTP Headers Attack の概要

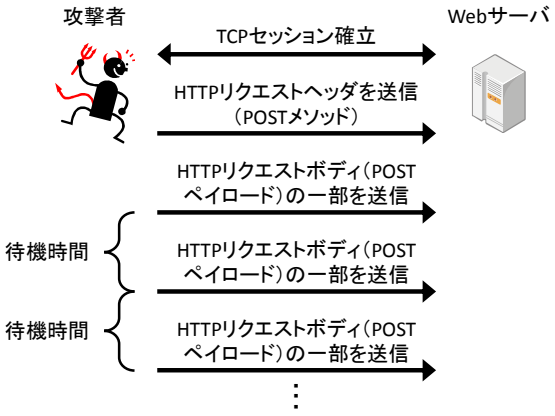

図2　Slow HTTP POST Attack の概要

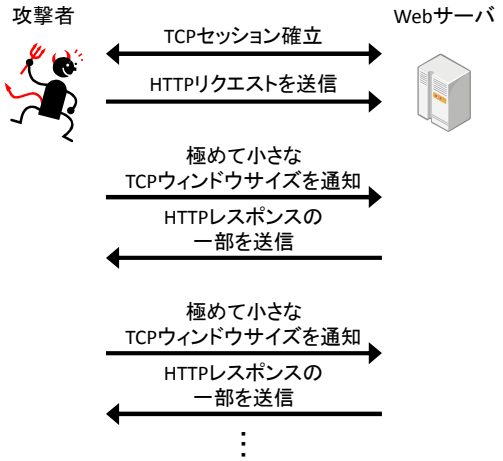

図3　Slow Read DoS Attack の概要

[i] https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf
[ii] https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read

インターネット上では、これらの攻撃手法を実装した攻撃ツールが複数公開されており、誰でも容易に攻撃を行うことが可能となっています。また、これらの攻撃を悪用した場合には、大量のパケットを送信する必要がないため、少人数による攻撃でも攻撃対象に深刻な影響を与える可能性があります。

警察庁では、Slow HTTP POST Attack を行う攻撃ツールが悪用された疑いがある攻撃事例を把握しています。

2 推奨する対策

Web サーバの管理者は、運用実態も十分に考慮した上で、必要に応じて Slow HTTP DoS Attack への対策を検討してください。考えられる対策の一例を表2に示します。

なお、Web サーバ等の設定変更内容によっては、正規の利用者の閲覧にも支障が発生する可能性があるため、事前に十分な検証を実施してください。

表2 Slow HTTP DoS Attack への対策例

対策内容	実施例	留意事項
HTTP リクエストヘッダ、リクエストボディにタイムアウト時間と最低受信レートを設定 （Slow HTTP Headers Attack、Slow HTTP POST Attack 対策）	Apache HTTP Server の mod_reqtimeout モジュール[i]で設定	回線速度が遅い正規の利用者に影響が及ばないように設定値は十分な検討、検証が必要である
HTTP リクエストボディのサイズを制限 （Slow HTTP POST Attack 対策）	Apache HTTP Server の LimitRequestBody ディレクティブ[ii]で制限	ファイルアップロード等を許可しているサーバでは制限することができない
異常に小さな TCP ウィンドウサイズを拒否	ファイアーウォール、UTM 等で設定	異常と判断する閾値の検討、検証が必要である
IP アドレス当たりの同時セッション数を制限		NAT やプロキシを経由して多数のユーザがアクセスする可能性も考慮する必要がある
攻撃を受けた場合に、攻撃元 IP アドレスからのアクセスを拒否		攻撃を事前に防ぐことはできない 攻撃者が IP アドレスを変更する可能性がある

また、多くの Web サーバプログラムでは、リクエストを全て受信した段階で、アクセスログが記録されます。このため、リクエスト受信が長時間に渡る Slow HTTP Headers Attack 及び Slow HTTP POST Attack では、攻撃に係るアクセスログの出力が大幅に遅延したり、攻撃が開始された時刻とログファイルに当該ログが書き出される時刻に差異が生じたりする場合があります。このため、攻撃が疑われる場合には、エラーログを確認する、ファイアーウォール等のログも確認するといった対応も必要となります。

[i] https://httpd.apache.org/docs/2.4/mod/mod_reqtimeout.html

[ii] https://httpd.apache.org/docs/2.4/mod/core.html#limitrequestbody