ログ解析メモ

平成２８年７月２７日

平成28年７月25日（月）

ほとんど　GET/wordpress/wp-login.php?[ランダム英字]=[ランダム英字]
（一般的には、ワードプレスの管理画面へのログイン試行のログ）

5:22:46　～　8:54:46　　94933回（毎秒 7.4回）　　585個はクローラボット
　うち　ステータス500　84914回　　263バイト　　応答　数秒～数十秒？
　　ステータス200　10012回　　2680バイト　　応答　2.2秒
　　（ログの記録時刻が前後していることから推測される事項）

一見、ワードプレス管理画面への侵入を試みているようにも見えるが、

Securi Blog の記事（平成28年６月27日）
Large CCTV Botnet Leveraged in DDoS Attacks（IoT防犯カメラによるBotNetを利用したDDoS攻撃）によると、同攻撃を受けたサーバのログに残されるリファラとして

http://engadget.search.aol.com/search?q=[ランダム英字]
http://www.google.com/?q=[ランダム英字]
http://www.usatoday.com/search/results?q=[ランダム英字]

が列挙されてたほか、

http://host-tracker.com/check_page/?furl=[ランダム英字]
http://jigsaw.w3.org/css-validator?uri=[ランダム英字]
http://validator.w3.org/feed/check.cgi?url=[ランダム英字]
http://www.facebook.com/l.php?u=[ランダム英字]
http://otaru-aq.jp/[ランダム英字]←対象ホストのＩＰ＋[ランダム英字]

が記録されていたことから、DDoS攻撃の手段として使用された可能性がある。