平成 28 年4月 28 日

インターネット観測結果等

（平成 28 年3月期）

- 宛先ポート 69/UDP に対するアクセスの増加
- Microsoft SQL Server を探索するアクセスの増加

1 宛先ポート 69/UDP に対するアクセスの増加

定点観測システムでは、3月 10 日以降、69/UDP を宛先ポートとするアクセスの増加を観測しました（図1）。69/UDP は、簡易なファイル転送を行うための通信プロトコルである TFTP において使用されるポートです。

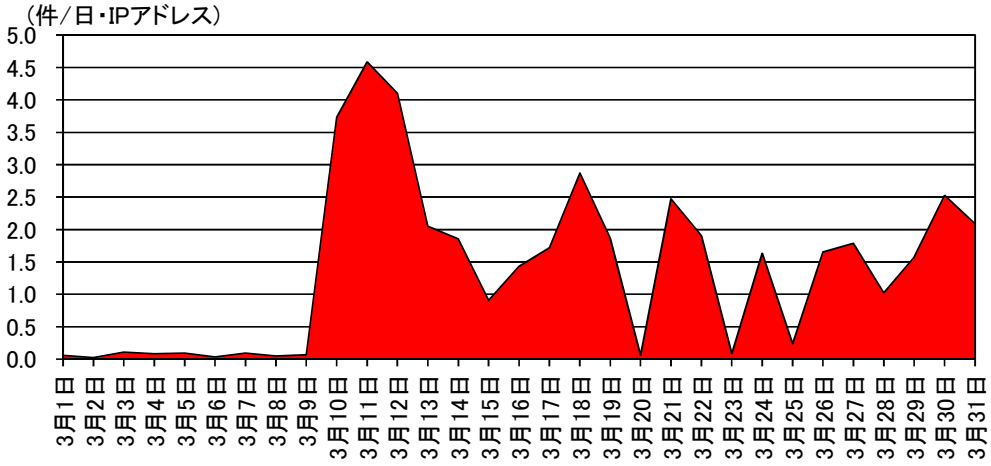

図1 宛先ポート 69/UDP に対するアクセス件数の推移

3月上旬に、英国のエディンバラ・ネピア大学のセキュリティ研究者のグループが TFTP を悪用するリフレクター攻撃の危険性を指摘する論文を発表[i]するとともに、同内容が多くのインターネットニュース等[ii]で取り上げられました。これらの内容によると、TFTP をリフレクター攻撃に悪用すると約 60 倍の増幅率があり、また、インターネット上には約 60 万の TFTP サーバが公開された状態にあると報告されています。

TFTP を悪用したリフレクター攻撃では、攻撃者が攻撃対象の IP アドレスに詐称し、TFTP サーバに存在するファイル名を指定してファイルの読み出し要求を送信すると、TFTP サーバは攻撃対象に指定されたファイルの送信を試みます。その際、ファイルは 512 バイトのパケットに分割して送信されますが、相手側から確認応答がないと、同一のパケットを何度か再送します（図2）。

[i] 「Evaluation of TFTP DDoS Amplification Attack」
https://researchrepository.napier.ac.uk/8746

[ii] 「600,000 TFTP Servers Can Be Abused for Reflection DDoS Attacks」
http://news.softpedia.com/news/600-000-tftp-servers-can-be-abused-for-reflection-ddos-attacks-501568.shtml

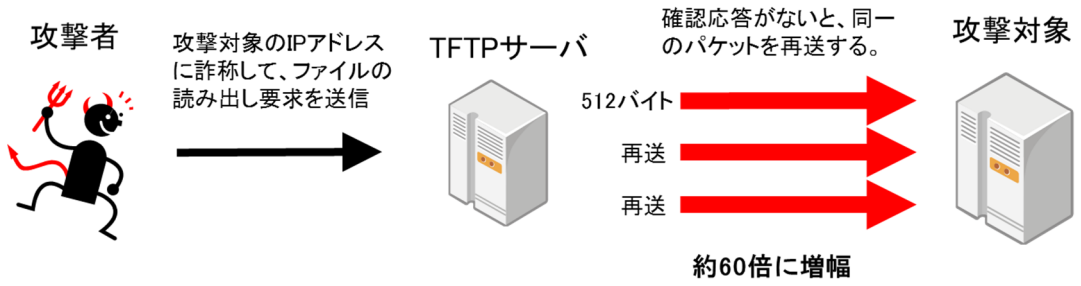

図2　TFTP を悪用したリフレクター攻撃

TFTP サーバがリフレクター攻撃に悪用されることを防ぐために、システム管理者は、TFTP サーバの状況を確認し、インターネットからの通信を遮断したり、適切なアクセス制限を実施するなどの対策が必要です。

2　Microsoft SQL Server を探索するアクセスの増加

定点観測システムでは、Microsoft SQL Server で使用される 1433/TCP を宛先ポートとするアクセスの増加を観測しました。1433/TCP に対するアクセスは、平成 27 年8月にも増加しており注意喚起[i]を実施しています。

観測したアクセスの内容を分析したところ、Microsoft SQL Server における PreLogin のパケットが増加していることが確認されました（図3）。

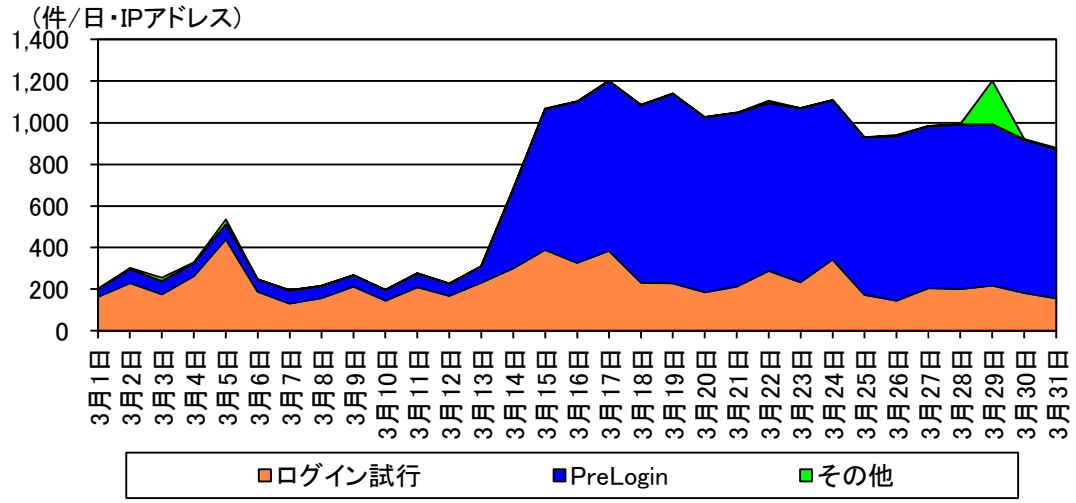

図3　宛先ポート 1433/TCP に対するアクセス件数の推移（リクエスト内容別）

PreLogin は、クライアントから Microsoft SQL Server へ接続する際に、クライアントがバージョン、暗号化等の情報を送信し、サーバもそれに応答して同様の情報を返すなどの処理を行うものです。

[i] 「Microsoft SQL Server を標的とするアクセスの増加について」（平成 27 年 10 月 28 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17082

そのため、これらの観測した PreLogin のパケットは、サーバの情報を取得するための探索行為と考えられます。

また、ログインの試行と考えられるアクセスも継続して観測しており、これらのアクセスは、ログインのユーザ名に管理用アカウントの「sa」を使用し、パスワードは未設定のものでした。

Microsoft SQL Server に対する探索行為が増加し、ログインを試行するアクセスも継続して観測していることから、システム管理者は以下の対策を実施することを推奨します。

- 管理用アカウントに適切なパスワードを設定する。
- インターネット側からアクセスする必要がない場合には、インターネットへの不要な公開を停止する。また、インターネット側からアクセスする場合には、不特定の IP アドレスからは接続できないように、適切なアクセス制限を実施する。