6X-03

ハニーポットによるパスワードスプレー攻撃のパターン解析とその対策

砂田　拳人†　　鳥居　直哉‡
創価大学　理工学部情報システム工学科†

1. はじめに

近年,リモートサーバ等へのパスワードクラックは巧妙になり，IDS 等では検知が困難になってきている．2018 年 3 月下旬に米国にて，数百校の大学システムがパスワードスプレー攻撃(以下 PSA)で不正侵入され，膨大な機密情報を窃取された[1]．2018 年 10 月には，Citrix Systems が PSA を受けている[2]．

PSA は複数のユーザに対して一つのパスワードを使用してログイン試行する攻撃である．攻撃者は，攻撃元 IP アドレス，攻撃時間，及び攻撃間隔を変更して攻撃する．そのため，正規ユーザとの見分けが困難となる．

本稿では，ハニーポット Cowrie を日本，米国，インドに設置し,2020 年 10 月 1 日から 2020 年 11 月 21 日の期間で日本，米国，インドでそれぞれ，178,718 回，221,627 回，及び 182,321 回のログイン試行を観測した．さらに，ログイン試行を解析することにより，PSA の攻撃パターンを考察し，対策を提案する．

2. PSA の抽出

本章では，Amazon が運営するクラウドサービス AWS[3]の日本，米国，インドのサーバに T-Pot[4]を設置した，T-Pot は，ドイツテレコムによって開発されたハニーポットで，19 種類のハニーポットを Docker 上で実装したハニーポットプラットフォームである．T-Pot のハニーポットのうちの Cowrie を使用して PSA 攻撃の抽出した．

2.1 ハニーポット Cowrie

Cowrie は低対話型のハニーポットで SSH や Telnet といったサーバを遠隔操作するためのソフトウェアに対する不正アクセスの情報のログを取得できる．Cowrie が出力するログの例を図 1 に示す．Cowrie では，アクセス時刻，ログイン試行時に使用した[user/password]が記録できる．ほかにも送信元 IP アドレス(srcIP)やその IP アドレスの国情報などが記録される．

Aug 11, 2020 @ 12:47:30.127	login attempt	[root/!@] failed
Aug 11, 2020 @ 12:47:31.169	login attempt	[root/!@] failed
Aug 11, 2020 @ 12:47:32.211	login attempt	[root/^%$#@!] succeeded
Aug 11, 2020 @ 12:48:04.143	login attempt	[uesr/user] failed
Aug 11, 2020 @ 12:48:05.276	login attempt	[admin/vertex25ektks123] succeeded

図 1　Cowrie から出力されるログ

2.2　抽出手順

Cowrie から取得したログから，次の手順により PSA を抽出した．まず，期間を設定する．例えば，1 日の場合には，2020/10/1 0:00 から 2020/10/2 0:00 と設定する．次に 1 つのパスワードに対して 10 種類以上の user へのアクセス試行があるログを PSA として抽出する．最後に抽出したログを可視化するために，縦軸に送信元 IP アドレスをとり，横軸にアクセス時刻としたグラフで表示する．

3. PSA の解析結果

本章では期間毎の抽出結果により分かった攻撃パターン，PSA で使用されたパスワード，srcIP，攻撃時刻の 3 点から解析する．観察期間での PSA 数は，日本 132 件，米国 308 件，インド 183 件，であった．

3.1 攻撃パターン

図 2 に縦軸に srcIP，横軸にアクセス時刻をとり，2020 年 10 月にインドで取得したログに対し，24 時間を単位で区切り PSA を抽出した結果を示す．攻撃パターンには(a)に示すようにに同じ送信元 IP アドレスから攻撃がくるパターンと，(b)に示すように一見まばらのように見えるが，ある時間帯に送信元 IP アドレスを変えて試行してくるパターンがある。図 3 に 3 日単位で抽出した結果を示す。図 3 から攻撃と攻撃の間に空白が見られる．PSA は 1 日かけて攻撃してくることはなく連続しても 2 時間程度であることが分かる．本節では，インドの抽出結果を示しているが，米国と日本でも同様の傾向があることが分かった．

Pattern analysis of honeypot password spray attacks and its countermeasures
Kento SUNADA†,　Naoya TORII†
†SOKA University

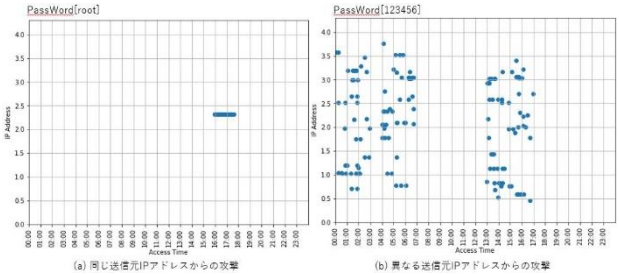

図 2　単位を 24 時間に設定した抽出結果

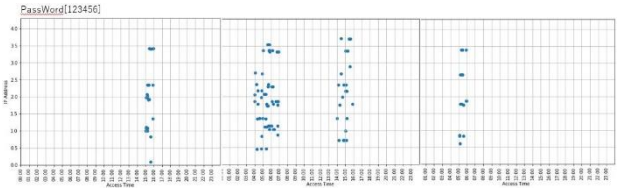

図 3　単位を 3 日に設定した抽出結果

3.2　使用されたパスワード

表 1 に国ごとの攻撃に使用されたパスワードを示す。使用された上位 3 位のパスワードは同じであった．ただし，インドだけは，2 位と 3 位が入れ替わっている．また，どのパスワードも予測が簡単なものになっている。

表 1　使用されたパスワード

順位	日本	米国	インド
1	123456	123456	123456
2	root	root	password
3	password	password	root
4	test123	password123	123
5	wasd	123	12345

3.3　送信元 IP アドレス

表 2 に srcIP の国情報を示す。どの国も上位 3 国は中国(CN)，米国(US)，及びフランス(FR)と同じになり，高い相関がみられた．

表 2　送信元 IP アドレスの国情報

順位	日本	米国	インド
1	CN	CN	CN
2	US	US	US
3	FR	FR	FR
4	GB	KR	IN
5	IN	BR	BR

3.4　攻撃時刻

図 4 に縦軸に 1 アクセスを 1 件とした件数をとり，横軸を現地時刻のアクセス時刻とした国ごとのグラフを示す．どの国も中国の IP アドレスからの攻撃が最大であることにより，中国の朝から夕方の時間帯に多くの攻撃が行われていることが分かる。また，平日と休日に分けて解析を行ったが，どの国も 1 日あたりの攻撃件数や，攻撃時刻にほとんど差はなかった．

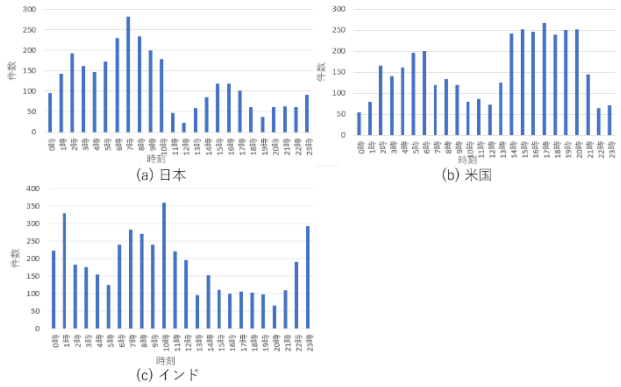

図 4　攻撃時刻(現地時刻)

4. 考察

日本，米国，及びインドへの PSA の共通点は，使用されたパスワード，srcIP の国情報の 2 点があげられる．異なる点は，攻撃件数，攻撃時刻の 2 点があげられる．

PSA の対策としては次の 2 点があげられる．第一に，どの国でも簡単で予測しやすいパスワードが攻撃に使用されているので，桁数が多い予測されにくいパスワードを設定する．第二に，中国の IP アドレスからの攻撃がどの国でも多く観測されているので，中国の IP アドレスからの通信で 1 時間程度の間に同じパスワードからのアクセスがある場合はその通信を遮断する．これらの対策は従来のパスワードクラックに対する基本的な対策であるため PSA に対しての有効な対策が今後の検討課題である．

5. まとめ

ハニーポットを日本，米国，インドの 3 国に設置し PSA について解析を行った．その結果，使用されたパスワード，srcIP の国情報には 3 国に高い相関がみられた．PSA への対策は PSA に有効な対策を示すことができず現状は従来のパスワードクラックに対する基本的な対策しかない．今後，IDS を使用した PSA の有効な検知方法について検討する．

参考文献

[1] ZDNet Japan,”『パスワードスプレー』攻撃に警戒を 日米で注意喚起,” https://www.cscd.osaka-u.ac.jp/user/rosaldo/031008cite.html(2018 年 4 月 4 日)
[2] TechTarget 「Citrix が『パスワードスプレー攻撃』で不正アクセス被害　なぜ防げなった？」 https://techtarget.itmedia.co.jp/tt/news/1908/22/news05.html(2019 年 8 月 22 日)
[3] AWS https://aws.amazon.com/jp/
[4] T-Pot https://github.com/telekom-security/tpotce