Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年 12 月 28 日

Topic

特定の IP 電話等交換機用のソフトウェアを標的としたアクセスの増加について

特定の IP 電話等交換機のソフトウェアを標的としたアクセスの増加を観測しています。アクセスの多くが当該ソフトウェアである Asterisk の管理用インターフェースに対するログインの試行と考えられることから、システムの管理者は適切な対策を行うことを推奨します。

1 特定の IP 電話等交換機用のソフトウェアを標的としたアクセスの増加について

IP 電話機等の回線交換を行う PBX[i]のオープンソースのソフトウェアである Asterisk では、管理や設定等を行うために、標準設定で 5038/TCP ポートが使用されます。

警察庁の定点観測システムにおいて、10 月末から、宛先ポート 5038/TCP に対するアクセスの増加を観測しています。増加したアクセスを分析したところ、Asterisk の管理用インターフェース[ii]にログインを試みるアクセスが多数を占めていました(図1)。

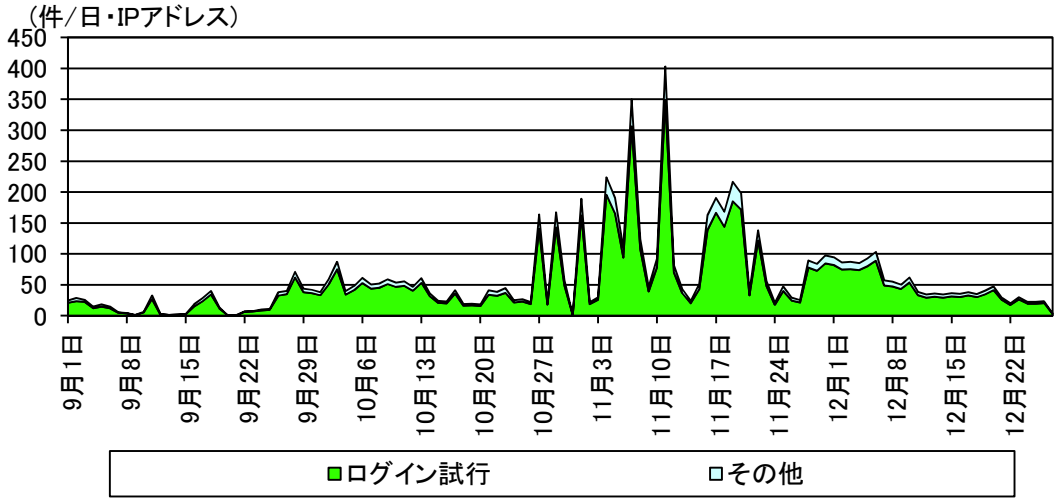

図1 宛先ポート 5038/TCP に対するアクセス件数の目的別推移(H27.9.1～12.27)

[i] PBX(Private Branch eXchange の略)とは電話機の回線交換を行う装置やソフトウェアのこと。
[ii] Asterisk Manager Interface(AMI)のことで、Asterisk の管理用インターフェースを外部へ提供するための API。

観測したアクセスの内容を分析したところ、ユーザ名及びパスワードの組合せを変えながらログインを試みるアクセスを多数確認しました（図2）。

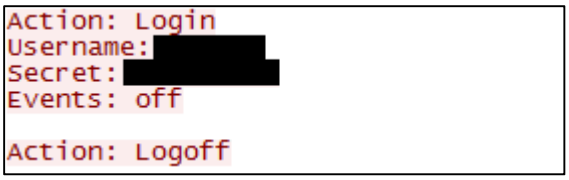

図2　管理用インターフェースにログインを試みるパケットの例

ユーザ名及びパスワードは、初期設定（デフォルト）のものや、単純な数字や単語が用いられていました。（表1）。

表1　観測したユーザ名及びパスワード(上位5位)

観測件数順位	ユーザ名	備考
1	admin	
2	manager	
3	test	
4	cron	
5	mark	デフォルト

観測件数順位	パスワード	備考
1	1234	
2	mysecret	デフォルト
3	password	
4	admin	
5	123456	

また、増加したアクセスの中には、ログインを試みるアクセスだけでなく、ログインと同時に設定ファイルの取得を試みるアクセスも確認しています（図3）。

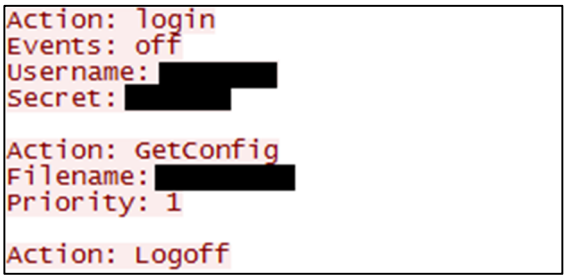

図3　管理用インターフェースにログインし、設定ファイルの取得を試みるパケットの例

2　対策

管理用インターフェースに不正にアクセスされるとデータの窃取や改ざん等を行われる危険性があります。過去には、セキュリティ対策が不十分な状態で Asterisk を利用していたため、第三者によって意図しない国際通話を行われてしまうなどの不正利用の被害を受けた事例[i]が公表されています。このため、管理者においては以下の対策を実施することを推奨します。

[i] 「不適切な設定で Asterisk を利用した場合に発生し得る不正利用に関する注意喚起」
https://www.jpcert.or.jp/at/2010/at100032.txt

- ログインに必要なパスワードを初期の設定から変更する。また、パスワードは、十分な強度があり、容易に推測できないものにする。
- 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。
- 外部に公開する必要がないサービスは、インターネットからの通信を遮断する。
- 使用している製品について最新のセキュリティ情報を確認し、必要に応じてソフトウェアのアップデートを実施する。