卒論(キーセンテンス)

> 1.序論

1.1 背景
IoTデバイスの普及により，IoTデバイスを対象としたマルウェアが急増している．ネットワークサービスを停止させる深刻な問題を引き起こしているマルウェアには，DDoS攻撃を行っているものが多く存在し，その対策が重要視されている．

1.2 IoTデバイスで検知を行う必要性
IoTデバイスでは放置された初期パスワードのままのアカウントや，保守されていないシステムの脆弱性をついた攻撃を行うため，侵入されてしまう．IoTデバイス上でマルウェアを検知をする事によってプロセスの挙動を知ることができ，未知のマルウェアを検知するのに有効である

1.3 マルウェア Miraiの概要
MiraiはTelnetログインが可能な端末を探索するスキャン活動があり，Telnetログインに成功した場合に，マルウェアをダウンロードさせ実行する．その後，C&Cサーバーから攻撃命令が来るとDDoS攻撃を行う．

1.4 研究目的
DDoS攻撃を行うマルウェアMiraiとその亜種の未知のマルウェアの検知

1.5 論文の構成
論文の構成を述べる．

> 2.関連研究

2.1 DDoS攻撃を行うマルウェアの分析
ハニーポットを用いてIoTマルウェア検体を収集し，収集したマルウェアをサンドボックス内で実行しその挙動を観測した研究がある．IoTマルウェアがDoS攻撃命令を受信するのは感染直後とは限らず，継続的に観測を行う必要があることがわかった．

2.2 動的解析によるマルウェア検知の研究
実行毎の挙動の差異に基づくマルウェアの検知手法では，同一のマルウェアを複数回実行した際の挙動の際を判断することによってマルウェア検知を行う．しかし，Miraiのように実行後に自身のバイナリファイルを削除してしまうマルウェアだと複数回実行することができず挙動の差異を判断することができないため マルウェアの検知が行えない問題がある．

> 3.提案手法

3.1 シンボルテーブルを用いた検知手法の提案

3.1.1 アプローチ
事前調査としてIoTデバイス上で普段の動作とマルウェアがダウンロードされ実行されたあとの動作の違いを明らかにする．実行コマンド，プロセスの2つのログデータの収集を行い，マルウェアが実行される前と後の相違点を明らかにする．

3.1.2 事前調査
Web上で公開されているMiariのソースコードを用いてマルウェアが感染する際の感染動作とC&Cサーバーとの通信が行われ，攻撃命令を待機するまでのマルウェアの動作を確認した．

3.1.3 シンボルテーブルを用いた検知手法の提案
プロセスの起動に用いられたバイナリファイルのシンボルテーブルからMirai独自の関数名を抽出し，その関数名を持つプロセスの動作を確認することでマルウェア感染の有無を判定する．

3.1.4 マルウェア探索動作による負荷と検知における制約事項
提案した検知手法は実行形式ファイルに含まれるシンボルテーブルの内容に基づいている為，マルウェアの実行形式ファイルに対して，stripコマンドを用いるなどしてシンボルテーブルが削除された場合には検知が行えないという課題がある．

3.2 システムコール呼び出し履歴を用いた検知手法の提案
3.2.1 新たな検知手法の必要性
システムコールを用いた検知を行うことによって，stripコマンドを用いてシンボルテーブルを削除したり，検知条件となっている関数名を変更するといった検知回避の対処がなされた場合でも検知が可能になる．

3.2.2 Miraiの特徴的な動作に基づく条件と検知条件
Miraiはインターネットに公開されているホストに対して新たな侵入先を見つけるためにTelnetログインが可能な端末をスキャンする活動を行っており，sendtoと呼ばれるソケットへメッセージを送るシステムコールを連続して呼び出していたことからsendtoに着目した検知条件を定める

3.2.3 誤検知の可能性
マルウェアではない正常なプログラムでも検知条件に一致して誤検知する場合がある．そのため，正常なプログラムが検知条件に一致するのか確認した．

3.2.4 システムコール呼び出し履歴を用いた検知手法の提案
システムコールの1つであるsendtoに着目をした検知手法のシステム概要について述べる．

> 4.評価実験

4.1 システムコール呼び出し履歴を用いた検知手法による定常的な動作負荷の評価
マルウェア探索動作によってIoTデバイス本来の動作が阻害されないことを評価するためにアンチウィルスソフトであるClamAVを動作させた状態のCPU，メモリ使用率を基準値として設定し，提案手法によるマルウェア探索動作の動作負荷について比較を行った

4.2 Miraiとその亜種マルウェアを対象とする判別性能評価
ハニーポットを用いて収集したマルウェアを用いて提案手法によるマルウェアの検知率を求める

5. 結論

5.1 まとめ
シンボルテーブルを用いた検知手法では，マルウェアの実行形式ファイルに含まれるシンボルテーブルを削除された場合には検知をすることができなかった．しかし，システムコール呼び出し履歴を用いた検知手法では，シンボルテーブルを削除された場合でもMiraiを検知することが可能だった．
(※以下の文はまだ評価を行っていないのどうなるかわかりませんがこのようなことを書こうと思っています)
ハニーポットを用いてマルウェアの収集を行い，収集したマルウェアをシステムコール呼び出し履歴を用いた検知手法で検知を行ったところ検知率は○%だった．

5.2 今後の展望
スキャン活動を行っていないbashliteと呼ばれるDDoS攻撃を行うマルウェアは検知を行う事ができないため，スキャン活動の他にも検知条件を定めてスキャン活動を行っていないマルウェアも検知できるようにする必要がある．