6W-01

Windows API コールログからのマルウェアの動作再現について

港　和人[†]　福田　洋治[†]　廣友　雅徳[‡]　毛利　公美[*]　白石　善明[††]
近畿大学[†]　佐賀大学[‡]　岐阜大学[*]　神戸大学[††]

1. はじめに

インシデント対応では，根絶と復旧の過程で，情報資産，ネットワーク構成，保存されているログに基づき，被害を受けた可能性のある端末や情報を洗い出し，影響の範囲を確定させるといった，証拠の収集，処理が行われる[1].

証拠の収集，処理の場面では，保存されたログの情報から，当時起こった事柄の再現，追跡が試みられることがあるが，インシデントにマルウェアを用いた攻撃が含まれる場合，特別な知識やスキルを持った人材が不足している組織では，マルウェアそのものを扱うことは被害の拡大や漏洩などの危険を伴う.

本稿では，マルウェアの実行解析の履歴（時系列の API コールのログ）から，その順番で API を実行するという，マルウェアの動作を再現するツールを提案し，試作したツールの動作確認を行った結果について述べる.

2. API コールログからのマルウェアの動作再現

API コールログを利用して，事後でも端末上で同様の動きを再現する，図 1 のような Windows API[2] を用いるマルウェアの API コールログを用いた動作再現ツールを提案する.

事前に対象のマルウェアを動的解析して，API コールログが得られていることを前提として，再現端末に本ツールを設置，動作させ，API コールログのファイルを与える.

API コールログのファイルから，記録された時刻順に 1 つずつログレコードを読み込み，以下の動作を繰り返す：（1）ログ抽出部は，1 つのログレコードから引数の文字列や API 名を抽出して，API 判別部で API，引数の型を判別する.（2）型変換部は，戻り値・参照データ管理部が保持するデータの型を当該 API の引数の型に変換する.（3）API コール部は，当該 API に引数を与えて呼び出し，戻り値や参照データを得ると，それを戻り値・参照データ管理部に渡す.

本ツールは，インシデント対応における調査活動を支援するためのフォレンジック支援のために，API コールログに従って，当時，呼び出された API を，時系列に忠実に呼び出し，当該プログラム（マルウェア）の動作を再現するものであり，端末に対する入出力，端末の状態などによって挙動を変えるようなプログラムには対応していない.

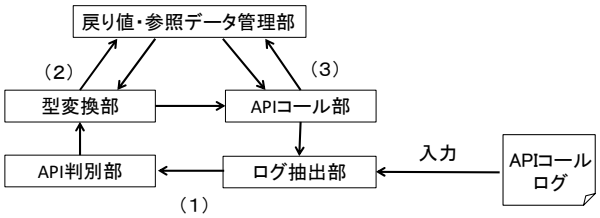

図 1　Windows API を用いるマルウェアの API コールログを用いた動作再現ツールの構成と動作

端末の入出力，状態によって挙動を変える処理の周辺の API コールログを複数パターン用意して，条件分岐の場所，条件を推測することで，同様の動きを再現することが考えられるが，今後対応を検討したい.

3. 試作と動作確認

Windows API を用いるマルウェアの API コールログを用いた動作再現ツールを C++言語を用いて試作し，これを用いて与えられた API コールログに従って各 API を実行できるかどうかを確認する実験を行った.

再現する対象の API は，システム・OS，ファイル・パス・ディレクトリ，通信のカテゴリの Win32API（CopyFile(), CreateFile(), CreateDirectory(), CreateDirectoryEx(), DeleteFile(), MoveFile(), MoveFileEx(), WriteFile(), InternetReadFile(), InternetOpen(), InternetOpenUrl(), HttpOpenRequest(), HttpSendRequest(), HttpQueryInfo(), InternetConnect(), InternetCrackUrl(), InternetSetOption(), InternetCloseHandle(), CloseHandle()）を想定して，ツールを試作した.

API コールログは，マルウェアの代わりに，指定した URL にアクセスして，ファイルを取得するという，単純な http クライアントを用意して，これを動作させ，API Monitor[4] というツールを使って，Win32API を観測，作成した.

試作したツールは，ノート PC(CPU: intel core i7 2.00GHz, Memory: 8GB, OS: Windows 10 Pro.

On Reproduction of Malware Behavior by Using WINAPI Call Logs
[†] Kazuhito MINATO and Youji FUKUTA, Kindai University
[‡] Masanori HIROTOMO, Saga University
[*] Masami MOHRI, Gifu University
[††] Yoshiaki SHIRAISHI, Kobe University

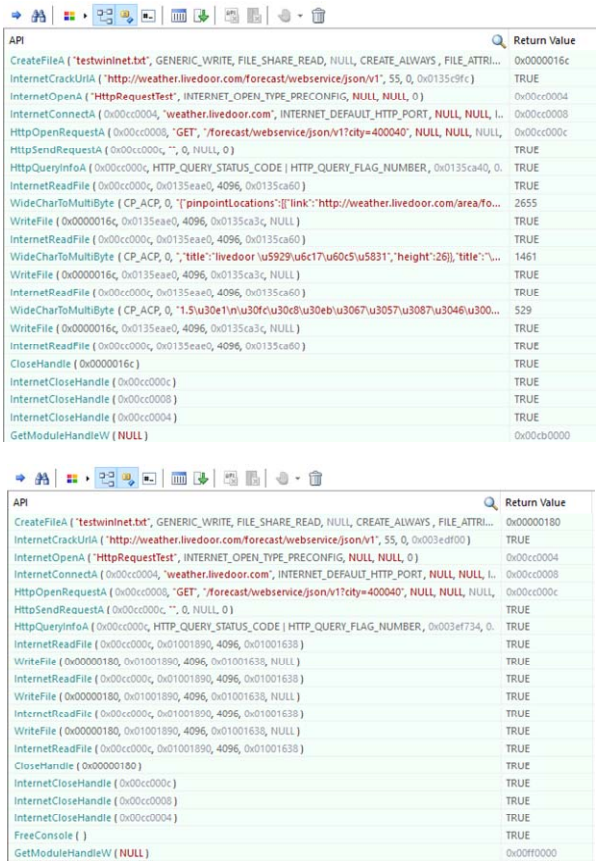

図2　API Monitor の画面の比較（上:入力で与えた API コールログ，下:試作したツールの API コールログ）

64bit)で動作させ，作成した API コールログのファイルを入力する．

API Monitor を動作させておき，試作したツールから呼び出される API を記録し，入力したファイルの内容と一致するかどうかを確認する．

試作したツールに入力した API コールログと，試作したツールの API コールログの API Monitor の画面を図 2 に示す．

API コールは，WideCharToMultiByte()を除いて，上下一致している．試作したツールの API コールログの中に WideCharToMultiByte()が含まれないのは，この API を呼び出せるようにツールに実装していなかったためである．

引数に与えるデータのポインタのアドレス，ハンドラなどは，API コールログの取得時と試作したツールによる再現時では，異なるが OS が動的にアドレスを割り当てているので，再現する上で問題にはならないと考えられる．

試作したツールは，一部のカテゴリに属する WIN32API を呼び出せるように実装したものであるが，他の WIN32API についても同様に実装することで，対応が可能と考えられる．

4. 関連研究

著者らはこれまで，インシデント対応における証拠の収集，処理の場面で，端末に履歴が記録されていないときに，通信パケットの記録から Web サイトを復元して，仮想環境の上で Web を介した攻撃を再現，端末で起こった事柄を観測することを支援するシステムを開発してきた[4]．

著者らのシステムを用いると，通信パケットの記録から Web を介した攻撃を再現して端末上で直接マルウェアを動作させるものであるが，提案するツールを用いることで，マルウェアそのものを扱うことなく，その影響を排除したかたちで，挙動の再現，観測を行うことが可能になると考えられる．

5. まとめ

マルウェアの実行解析した API コールログから，ログに記録された順番で API を実行し，動作を再現するという，マルウェアの動作再現ツールを提案し，これを試作して意図した動作をすることを確認した．

本ツールの動作は，API コールログから，ログレコードを 1 つずつ読み込み，当該 API の呼び出すという単純なものであるが，今後，ステップ実行や逆再生，動作の可視化の機能を含めることを考えている．

マルウェアそのものを扱うことなく，端末でその動作を再現，起こった事柄を観測するという用途の他に，例えば，再発防止の場面で，端末で当該マルウェアと同じ動きを AMS で検知できるかテストし，対応状況を確認するといった用途も考えられる．

参考文献

1) 寺田真敏：組織のセキュリティ文化を反映するシーサート活動，情報管理，vol.59, no.2, pp.96-104（2016 年 5 月）．
2) Microsoft：Windows API Index，入手先＜https://msdn.microsoft.com/ja-jp/library/windows/desktop/ff818516(v=vs.85).aspx＞（参照 2018-01-03）．
3) Rohitab Batra：API Monitor，入手先＜http://www.rohitab.com/apimonitor＞（参照 2018-01-03）．
4) 奥田裕樹，福田洋治，白石義明，井口信和：ドライブ・バイ・ダウンロード攻撃によるインシデントを再現するフォレンジック支援システム，信学技報（ICSS），Vol.117, No.125, pp.81-86（2017 年 7 月）．