SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

フォレンジック調査の補助のための Windows API コールログを用いた不正プログラムの動作再現ツール

A Reproduction Tool of Malicious Programs Behavior by Using WinAPI Call Logs for Supporting Digital Forensic Investigation

松田 尚也* Naoya Matsuda
福田 洋治* Youji Fukuta
廣友 雅徳† Masanori Hirotomo
白石 善明‡ Yoshiaki Shiraishi

キーワード フォレンジック調査，動作再現，不正プログラム，Windows API コールログ

あらまし

Windows API は，Windows の OS がアプリケーション等のプログラムに対して公開しているインターフェースであり，プログラムから直接呼び出すほかライブラリやフレームワークを介し間接的に呼び出すことで OS が提供する機能を利用することができる．Windows API コールログは，ある 1 つのプログラムを実行させたときに呼び出される Windows API 名，引数，戻り値を，特殊なツールを使って取得し時系列に記録した履歴情報であり，プログラムの主要な動作を表している．

Cao らは，ホストイベントやネットワークがシミュレートされている仮想マシン内でプロセスを監視，Windows API コールログを取得し，その情報に基づいてマルウェアの可能性のあるものを捉え，動的解析を支援するシステムを提案している[1]．Shosha らは，静的プログラム解析により抽出した機械語命令のうち Windows API コールの引数の欠損部分をプロセスのプログラムを再構築することで推測しプロセスの動作把握を補助する手法を提案している[2]．

本研究では，現在残されている状況を調べ当時何が起こったのかを証拠に基づいて確定させるフォレンジック調査を補助するための，Windows API コールログを用い記録された順序で各 Windows API を呼び出すことで当該プログラムの動作を再現するツールの検討，試作と評価実験を行っている．インシデント発生時，被害ホストやその周辺機器にログが残り，これらに対してフォレンジック調査が実施されることがあるが，どんな攻撃が行われたのか，どんな不正プログラムが実行されたのか，把握が困難な場合がある．予め複数の不正プログラムの Windows API コールログを用意し，本ツールを使用することでプログラムの動作を再現して，被害ホストやその周辺機器と同じ環境，条件で取得したログと，残っていたログを比べ，類似するものを当時実行されたものとして推測できるようになると考えられる．

参考文献

[1] Ying Cao, Qiguang Miao, et.al, "Osiris: A Malware Behavior Capturing System Implemented at Virtual Machine Monitor Layer," 2012 Eighth International Conference on Computational Intelligence and Security, Guangzhou, pp.534-538, Dec. 2012.
[2] Ahmed F. Shosha, Lee Tobin, Pavel Gladyshev, "Digital Forensic Reconstruction of a Program Action," 2013 IEEE Security and Privacy Workshops, San Francisco, CA, pp.119-122, May. 2013.

* 近畿大学，東大阪市，Kindai University, 3-4-1 Kowakae, Higashi-Osaka-shi, 577-8502 Japan
† 佐賀大学，佐賀市，Saga University, 1 Honjo-machi, Saga-shi, 840-8502 Japan
‡ 神戸大学，神戸市，Kobe University, 1-1 Rokkodai-cho, Nada-ku, Kobe-shi, 657-8501 Japan