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

準パススルー型ハイパーバイザを用いて取得したメモリデータの分析

Analysis of Memory Data Acquired Using a Parapass-through Hypervisor

大森貴通* 平野学* 小林良太郎†
Takamichi Omori Manabu Hirano Ryotaro Kobayashi

キーワード ランサムウェア，マルウェア，仮想化，メモリフォレンジック

あらまし

ランサムウェアの被害が拡大しており，社会インフラや病院などの公共サービスの停止を余儀なくされるケースが増えている．我々の先行研究[1]では，従来のシグネチャ手法では検知の難しかった新種や亜種のランサムウェアの検知を目的とする振る舞い型の手法を提案した．提案手法は図１に示すように仮想化基盤ソフトウェアであるハイパーバイザを振る舞いデータの収集に利用しており，オペレーティングシステムで動作するメインの検知機能が回避または無効化された際の次の防御層として機能することを想定している．提案手法は軽量のハイパーバイザである BitVisor[2] を採用してランサムウェアのストレージ装置へのアクセスパターンを取得，監視マシンへネットワーク経由で転送する．ストレージ装置のアクセスパターンから特徴量を抽出し，機械学習によってモデル化することで，良性プログラムと悪性プログラム（ランサムウェア）を判別する．先行研究[3]では振る舞い型の検知に利用できるストレージアクセスパターンのデータセットを公開した．データセットは７種のランサムウェアと５種の良性プログラム（Zip 圧縮，暗号化など）から構成され， 例えば Sodinokibi (REvil) については過去２年間の１７種の変異種について振る舞い型の検知が可能であることを示した．

先行研究[1, 3]ではハイパーバイザから得た低レベルのストレージ入出力パターンだけを使ってランサムウェアの脅威を検知できることを示した．しかし，複数のプロセスのアクセスが重なったときや，BitLocker ストレージ暗号化を有効にした時に特徴量が大きく変化し，検知性能が著しく低下することを確認した．そこで，本研究では，ストレージアクセスパターンに加え，ハイパーバイザで RAM のデータを取得し，低レベルの情報だけを用いて，プロセスの振る舞いを推定できると考えた．本稿ではランサムウェアの実行前後で RAM のメモリダンプを取得し，4 KiB ページ単位での同一のページ数の変化ならびにエントロピーの変化について分析した結果を報告する．

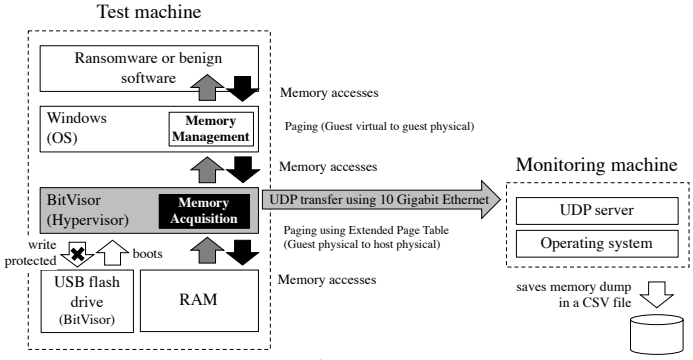

図１: ハイパーバイザを用いた監視システム

参考文献

[1] Hirano, M., Kobayashi, R., “Machine learning based ransomware detection using storage access patterns obtained from live-forensic hypervisor,” Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, pp. 1–6, 2019.

[2] Shinagawa, T., Eiraku, et al., BitVisor: A Thin Hypervisor for Enforcing I/O Device Security, in: Proceedings of the 2009 ACM SIGPLAN/SIGOPS international conference on Virtual execution environments (VEE 2009), pp. 121–130, 2009.

[3] Manabu Hirano, Ryo Hodota, Ryotaro Kobayashi, “RanSAP: An Open Dataset of Ransomware Storage Access Patterns for Training Machine Learning Models,” Forensic Science International: Digital Investigation (accepted, to appear).

* 豊田工業高等専門学校 情報科学専攻, 愛知県豊田市栄生町 2-1
† 工学院大学，東京都新宿区西新宿 1-24-2