5ZA-04

ランサムウェア暗号化攻撃遅延とメモリ領域局所化を利用した鍵回復手法の初期検討

樋口諒† 稲村浩† 石田繁巳†
†はこだて未来大学

1 はじめに

近年，ランサムウェアによる被害が増加しており，脅威となっている．警察庁によると，令和5年における企業や団体に対するランサムウェアによる暗号化攻撃は197件発生しており，令和4年上半期以降で高い水準で推移している [1]．ランサムウェアによる暗号化攻撃は企業や団体の大小に関わらず被害を与えている．

ランサムウェア暗号化攻撃への対策の1つとして，バックアップの利用があげられる．しかし，バックアップにより完全に復元できたケースは少ない [1]．

本研究ではバックアップに依らない復元手法の実現を目的とする．バックアップに依らない手法として，メモリフォレンジックによる鍵回復手法が存在する [2]．メモリフォレンジックによる鍵回復手法ではランサムウェアの動作中にメモリダンプし，取得したメモリイメージから鍵を探索して取得する．この手法では，鍵がメモリ上に存在するタイミングでメモリダンプする必要があるため，そのタイミングや取得頻度が重要となる．

提案手法では，囮ファイルを用いてランサムウェアプロセスの検知・特定することにより，探索するメモリ領域の局所化と，CPU使用率の制限を行う．これにより，メモリ上に鍵が存在する時間を引き延ばしメモリダンプ処理の軽量化によってメモリフォレンジックによる鍵回復の確実性の上昇を目指す．

2 関連研究

囮ファイルを利用して暗号化攻撃の検知と遅延を行う研究として，田中らは大量の囮ファイルにより暗号化攻撃を遅延させる研究を行った [3]．囮ファイルとは，正規のアクセスはないという前提をおいたファイルのことであり，囮ファイルにアクセスしたプロセスはランサムウェアであると仮定できる．

メモリフォレンジックにより暗号鍵を回復する研究として，Daviesらはランサムウェアを解析し，タイムラインを作成することでメモリダンプを行うタイミングを推定し，鍵の探索を行った [4]．しかし，この手法では未知のランサムウェアに対してメモリダンプするタイミングを推定できない．

3 提案手法

本研究では，囮ファイルの監視によりランサムウェアプロセスの検知・特定後に，鍵探索すべきメモリ領域を局所化し，特定したランサムウェアプロセスのCPU使用率を制限することで暗号化処理を遅延させる．特定したプロセスが使用している領域のみにメモリ領域を局所化することにより，単位時間あたりのメモリダンプの回数を増やす．PIDを指定してプロセスのCPU使用率を制限することによりランサムウェアプロセスの実行速度を低下させて暗号鍵がメモリ上に存在する時間を引き延ばす．これら2つの手法は，メモリダンプ可能な時間を延伸させるとともに単位時間当たりの取得回数も増やし，メモリフォレンジックによる鍵回復の確実性を高める．提案手法の流れを図1に示す．

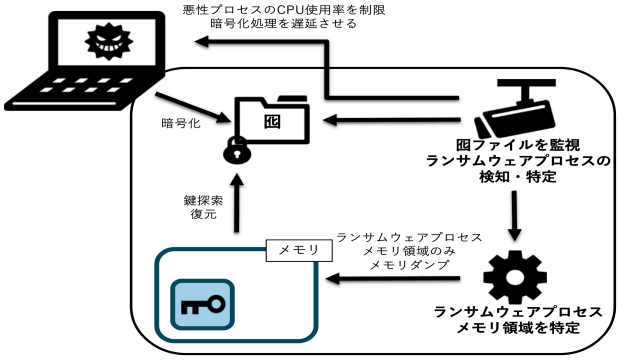

図1: 提案手法概要図

本手法では対象のランサムウェアに固有の情報や鍵がメモリに存在するタイミングの推定などは行わないため，未知のランサムウェアにも対処可能である．

3.1 実装

本研究では，実装と評価にLinux環境を想定している．囮ファイルのファイルサイズは既存研究にて用いられた2KBに設定した [3]．囮ファイルの監視にはeBPF

Initial Study of Key Recovery Method Using Delayed Ransomware Encryption and Localized Memory Region

Ryo Higuchi†, Hiroshi Inamura†, Shigemi Ishida†
†Future University Hakodate, Japan
†{b1020239, inamura, ish}@fun.ac.jp

を利用する．その際に，囮ファイルへの削除操作をトリガーとして検知し，削除操作したプロセスをランサムウェアプロセスとする．ランサムウェアプロセス特定後に，ランサムウェアプロセスの CPU 使用率の制限と，ランサムウェアプロセスが使用しているメモリ領域を特定し取得するメモリを局所化する．CPU 使用率の制限には，cgroup-v2 を利用した．メモリ局所化では，/proc ディレクトリに存在するプロセスごとに管理されたメモリ情報を基にプロセスのヒープ領域とスタック領域のみのメモリダンプを行った．取得したメモリイメージを鍵長幅でスライドさせながら切り出したものを候補鍵とし，総当たりで復号を試みる．復号の成功は囮ファイルの平文との一致で判断し，攻撃に用いられた暗号鍵を特定する．

4 評価

提案手法の初期的評価として実験を行う．評価では，探索するメモリ領域を局所化することによる復元の成否と，探索に必要なメモリ領域サイズを示した．メモリ局所化を行った上で，CPU 使用率の制限によるメモリダンプの実行回数の変化と復元の成否を比較した．評価には暗号化操作を模した擬似ランサムウェアを用いた．局所化していないメモリ領域のダンプには LiME（Linux Memory Extractor）を用いて行った．LiME は，Linux のカーネルモジュールとして動作し，物理メモリ全体のダンプを行う．暗号方式は AES とし鍵長は 256bit とした．

4.1 評価環境

ホスト OS の Windows11 上に VirtualBox によって Ubuntu 22.04 を仮想マシンとしてインストールし実験を行った．仮想マシンには 4GB のメモリ，1 つのコアを割り当てた．擬似ランサムウェアの暗号鍵は変更されないものとした．実験では，ファイルサイズが 2MB のファイルを 10 個と，囮ファイル 1 個を，暗号化を行った．

4.2 評価結果

4.2.1 メモリ領域局所化の評価

表 1 に，メモリダンプ 1 回当たりのダンプファイルのサイズ，復元の可否を示す．メモリ領域の局所化によりダンプファイルサイズには大きな違いがみられた．LiME ツールによるメモリダンプはダンプファイルサイズが大きいため，メモリダンプに時間がかかり，暗号化処理中に完了しなかった．暗号鍵の探索に関して，今回はダンプしたメモリを総当たりで鍵探索を行っているため，計算量はダンプファイルサイズに依存する．以上から，メモリ局所化によりメモリダンプの試行回数の増加と，鍵探索における計算量の削減を行うことができる．

表 1: メモリ局所化

使用ツール	ダンプファイルサイズ	復元の可否
提案手法	12.132MB	可
LiME	2.0GB	不可

表 2: CPU 使用率制限による効果

CPU 使用率 (%)	復元可否	ヒープ領域取得回数	スタック領域取得回数
100	可	1	0
80	可	1	0
60	可	3	2
40	可	5	4
20	可	6	5
10	可	23	22
1	可	215	215

4.2.2 CPU 使用率制限の評価

表 2 に，ランサムウェアプロセスの CPU 使用率の上限，復元の可否，ヒープ領域取得回数，スタック領域取得回数を示す．CPU 使用率の上限を制限することにより，メモリダンプの回数は大きく変化した．今回は CPU 使用率の制限による復元の可否に変化はみられなかった．しかし，鍵を複雑に隠匿するランサムウェアに対しては CPU 使用率を制限し，メモリダンプの回数を増加させることは鍵探索の情報を増やすこととなり有効となると考えられる．

5 おわりに

本稿では，メモリフォレンジックによる鍵回復を確実なものにするために，ランサムウェアプロセスの CPU 使用率の制限と探索するメモリ領域の局所化による有効性を確認した．結果として，メモリ局所化はダンプ処理と鍵探索処理の軽量化に有効的であった．メモリ局所化のもとでの CPU 使用率の制限は復元の可否に違いは見られなかったが，メモリダンプの取得回数が増加したため，鍵回復の確実性を向上できた．これにより，ランサムウェア暗号化プロセスの詳細な分析することが可能になると考えられる．

参考文献

[1] 警視庁: 令和 5 年におけるサイバー空間をめぐる脅威の情勢等について, https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf, Accessed on March, 2024.

[2] 竹林康太, 上原哲太郎, 佐々木良一 他: ライブフォレンジックを用いた暗号化ファイル復号技術の開発, 研究報告マルチメディア通信と分散処理 (DPS), Vol. 2015, No. 38, pp. 1–6 (2015)

[3] 田中智也, 小池一樹, 小林良太郎, 加藤雅彦 他: ダミーファイルを利用した暗号化型ランサムウェア対策システムの実装, コンピュータセキュリティシンポジウム 2019 論文集, Vol. 2019, pp. 163–169 (2019)

[4] Davies, S. R., Macfarlane, R., and Buchanan, W. J.: Evaluation of live forensic techniques in ransomware attack mitigation, Forensic Science International: Digital Investigation, Vol. 33, p. 300979 (2020)