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

ランサムウェアの解析とその対策に関する研究
Research on the analysis of ransomware and its countermeasures

古門良介 * Ryosuke Kokado
池上雅人 † Masato Ikegami
住田裕輔 † Yusuke Sumida
岡庭素之 † Motoyuki Okaniwa
白石善明 * Yoshiaki Shiraishi
森井昌克 * Masakatu Morii

キーワード マルウェア ランサムウェア

あらまし

本研究ではユーザにとって利用が容易で，かつ従来よりランサムウェア感染後にいち早く検知し，完全な復旧を目的として，より精度の高いファイル復旧方法を提案する．

提案方法としては，既存のランサムウェア検知手法に対して 2 つの異なるしきい値を設け積極的な介入（プロセスの強制終了）と控えめな介入（ランダムなファイル暗号鍵生成の阻止）とで動作を切り替えることを行い，ファイル暗号化鍵に対してもその制御に介入し，制御した鍵による復旧に取り組む．

提案手法

既存のランサムウェア検知手法として利用した Scaife らによる CryptoLock[1] はファイルイベントごとに，ファイル類似度・ファイル拡張子とファイルシグネチャの一致・シャノンエントロピーの増減によってプロセスごとにスコアリングする．

本研究では，新たに検知のしきい値を FN (ランサムウェアを検知できないケース) を最小限となる T_1，FP (正常プロセスをランサムウェアと検知するケース) を最小限となる T_2 を設けた．

したがって従来手法のしきい値 T_B との関係は以下となる．

$$T_1 < T_B \leqq T_2$$

T_1 時に DLL インジェクションすることでランダムなファイル暗号鍵の生成を任意の鍵への生成にすり替えた．T_2 時には対象プロセスを強制停止を行う．また，同プロセスに対してメモリダンプを取得し，暗号鍵の捜索をし，検知までの時間差で暗号化されたファイルの復旧を行う．

最初の介入の基準値が従来よりも低いので従来に比べて検知までの時間差は減り，暗号化によって喪失するファイル数を減らすことが可能となる．

表 1: 介入手法の比較

介入手法	ユーザ体験への影響	ファイル復旧難易度
介入なし	なし	高
ランダムな暗号鍵生成の阻止	低い	中（鍵は把握できるが暗号化は進行）
プロセスの強制終了	大きい	低（終了後は暗号化が止まるため）

謝辞

本研究は，総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」 の成果の一部である．

参考文献

[1] Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin R. B. Butler. Cryptolock (and drop it): Stopping ransomware attacks on user data. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, pp. 303–312, 2016.

* 神戸大学大学院工学研究科電気電子工学専攻，神戸市
† キヤノン IT ソリューションズ株式会社 IT プラットフォーム技術統括本部サイバーセキュリティ技術開発本部サイバーセキュリティラボ, 東京都港区