東京大学
情報理工学系研究科 電子情報学専攻
修士論文

Fuga: ランサムウェアからリアクティブにデータを保護するシステムの設計と実装

Fuga: Design and Implementation of
Reactive Data Protection System against Ransomware

48-236427
手塚 尚哉
Naoya Tezuka

指導教員　落合秀也 准教授

2025 年 1 月

概要

ランサムウェアの脅威に対応するためには，ランサムウェアの活動を迅速に検知して被害の拡大を防ぐだけでなく，仮に被害を受けた場合でもデータを復旧することができる手法が必要となる．定期的なスナップショットによる復旧は一般的な手法だが，バックアップの粒度の粗さから頻繁な取得は難しく，その結果データ損失が発生するおそれがある．本研究ではランサムウェアのファイル侵害の直前にデータを隔離領域へ退避させることでデータ復旧を実現するシステム Fuga を提案する．Fuga はファイル単位のバックアップをリアクティブに取得することでスナップショット方式の課題を克服し，誤検知時のコストも軽減する．本稿では Fuga の設計を行い，ランサムウェアのファイル侵害方法に応じた実装方針を示した．さらに eBPF を用いた実装を行い，様々なファイルサイズにおけるデータ保護性能とオーバーヘッドを評価した．これにより，ランサムウェアからデータを保護するシステムとして Fuga が実用的であることを示した．

Abstract

To address the threat of ransomware, it is essential not only to detect ransomware activities quickly to prevent further damage, but also to have methods for recovering data in case the attack succeeds. While recovery using periodic snapshots is a common approach, their coarse granularity makes frequent backups impractical, increasing the risk of data loss. In this study, we propose Fuga, a system that ensures data recovery by evacuating data to an isolated storage area just before ransomware compromises files. Fuga reactively performs file-level backups, addressing the limitations of snapshot-based approaches while reducing the cost of false positives. We presented the design of Fuga and its implementation strategies tailored to different methods of ransomware file compromise. Furthermore, we implemented Fuga using eBPF, and evaluated its data protection performance and overhead across various file sizes. conducted evaluation experiments. The results demonstrate that Fuga is effective and practical as a data protection system against ransomware.

目次

図目次

表目次

第 1 章

序論

これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．

これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．

これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．

これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．

これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．これは，序論の文章である．

参考文献を引用してみる [?, ?]．もうひとつ引用する [?]．日本語の文献 [?, ?] も引用する．創造情報学専攻のウェブページを引用する [?].

第 2 章

ランサムウェア

2.1 概要

ランサムウェアとはマルウェアの一種であり，攻撃者が要求した金額が支払われるまで，システムやデータへのアクセスを制限する．言い換えると，データや計算資源，サービスなどのリソースを人質に取って被害者を脅迫することで身代金を要求するマルウェアがランサムウェアである．

ランサムウェアはリソースへのアクセスを制限する方法に基づいて暗号化ランサムウェアとロッカーランサムウェアに分類される [4]．暗号化ランサムウェアは感染先ホストのファイルやデータを暗号化し，元のファイルを削除または上書きする．ロッカーランサムウェアは暗号化を行わず，デスクトップのスクリーンやブラウザをロックすることで被害者がシステムを利用できないようにする．本研究は暗号化ランサムウェアを対象としているため，本稿では暗号化ランサムウェアを単に「ランサムウェア」と呼ぶことにする．

図 2.1 に示すように，AIDS Trojan [5] は 1989 年に最初のランサムウェアとして登場した．AIDS Trojan は被害者に郵送されたフロッピーディスクを介して感染し，Windows システムを対象としていた．その後インターネットの普及に伴い，ランサムウェアによる被害が増加し始めた．2005 年に登場した GPCode [6] はフィッシングメールを介して感染し，独自の暗号化アルゴリズムによってファイルを暗号化した．

現代のランサムウェアはますます高度化している．ランサムウェアの進化における重要な要素を以下に列挙する．

- AES などの対称鍵暗号化アルゴリズムや RSA，楕円曲線暗号などの非対称鍵暗号化アルゴリズムを使用して暗号化を行うようになっている [1]．これにより，復号鍵を入手することができなければデータの復号はほぼ不可能となった．
- Windows だけでなく，Linux，macOS，Android などの他の OS を対象としたランサムウェアも登場するようになった．
- ビットコインに代表される仮想通貨が普及したことで身代金の支払いが匿名で行えるようになり，攻撃者の特定が難しくなった．

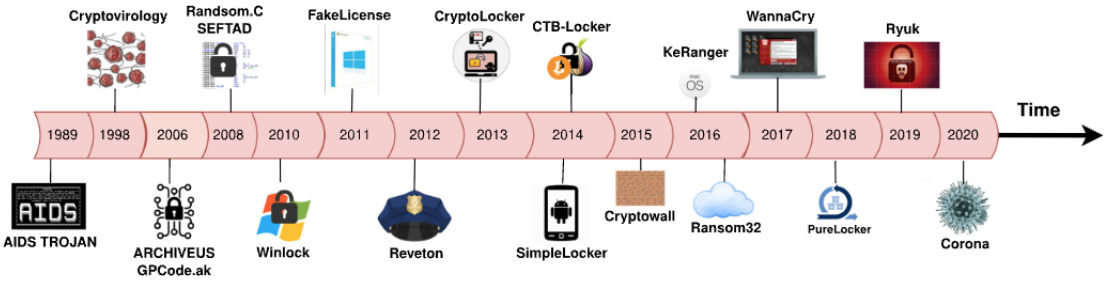

図 2.1. Development of major ransomware families (1989–2021). The first know ransomware, AIDS Trojan, was introduced in 1989. [1].

- ランサムウェアの開発と配布を有料で行うサービスである Ransomware as a Service (RaaS) が登場し，専門知識が無くとも容易に攻撃を実施することができるようになった．
- 無差別的な攻撃から，特定の高価値な組織 (政府機関や大企業など) を対象とした高度な攻撃に移行しつつある [7].

2.2 ランサムウェアの分類

2.2.1 悪意ある振る舞いに基づく分類

2.1 節で述べたように，ランサムウェアは被害者が身代金を支払うまでリソースへのアクセスを制限するが，アクセスを制限する方法には多様性が見られる．本稿では Oz らの分類 [1] を参照し，その方法として**暗号化**，**データ破壊**，**データ窃取**を扱う．

暗号化：ランサムウェアは暗号化鍵を用いてデータを暗号化し，元のデータを削除するか，暗号化後のデータで上書きする．この時使用する鍵はランサムウェアの実行ファイルに埋め込まれているか，感染先ホスト上で生成されるか，C2 サーバとの通信から取得されるかのいずれかである．ファイルを暗号化するランサムウェアの中には，暗号化の対象とするファイルを限定するものも存在する．例えば CTB-Locker [8] は，被害者にとってより高価値なファイルのみを暗号化するために，.pdf や.zip などの拡張子を持つファイルを暗号化対象としている．また，Jigsaw [9] は 10MB 以下のファイルのみを暗号化する．このように，ランサムウェアの一部は暗号化の対象とするファイルを限定することで，ランサムウェアの活動が検出されるリスクを緩和している [10] と考えられる．

データ破壊：破壊活動を目的としているがランサムウェアに擬態して攻撃者の意図を隠蔽しようとするマルウェアが確認されている．例えば，2017 年に発見された NotPetya [11] は，ハードディスク全体を暗号化した後，ビットコインの送金先として無効なアドレスを提示していた．このアドレスはランダムに生成されており，攻撃者が金銭を回収する意図がないことから，NotPetya は破壊活動を目的として作成されたと考えられる [11]．同様の攻撃として，暗

号化を行わず，ランダムなデータでファイルを上書きするマルウェアを作成し使用することも可能である．なお，このタイプのマルウェアの被害者は身代金を支払ってもリソースを復旧することができないが，本研究ではランサムウェアとして扱う．

データ窃取：ランサムウェアは機密文書や顧客の個人情報などの重要データを摂取する可能性がある．データの暗号化または破壊とデータの窃取を組み合わせて脅迫を行うランサムウェアを「二重脅迫ランサムウェア」と呼ぶ．二重脅迫ランサムウェアは，データの復旧のために一回，窃取したデータの公開を防ぐためにもう一回，被害者に身代金を要求する．二重脅迫ランサムウェアによる被害は近年増加しており，SOPHOS 社が発表したレポート [12] によると，2023 年に発生したランサムウェアインシデントのうち 32% においてデータの摂取も発生している．加えて，データの窃取のみによって脅迫を行う「ノーウェアランサム」[13] と呼ばれる手法も確認されている．

2.2.2　暗号化アルゴリズムに基づく分類

データを暗号化するランサムウェアは，ISO/IEC [14] などの標準化団体が採択した標準的なアルゴリズムを使用する場合と，攻撃者によって独自に設計された暗号化アルゴリズムを使用する場合がある．Begovic ら [2] が調査した，1991 年から 2021 年までに確認された著名なランサムウェア変種の暗号化アルゴリズムの使用状況を**図 2.2** に示す．**図 2.2** によると 8.2% のランサムウェアが独自の暗号化アルゴリズムを使用しているが，近年のランサムウェアは AES や RSA といった標準的な暗号化アルゴリズムを使用する傾向が強いことがいくつかの先行研究 [1, 15] にて指摘されており，この数値には初期のランサムウェアが多く含まれていると考えられる．より具体的には，攻撃者が独自に設計した暗号化アルゴリズムは強度が不十分で暗号解読者による解読が容易であることが多い [15] ため，2000 年代後半から 2010 年代前半にかけて，十分に評価され強度が高い暗号化アルゴリズムが採用されるようになっていった [1].

ランサムウェアは**対称鍵暗号化**，**非対称鍵暗号化**，**ハイブリッド暗号化**のいずれかの暗号化技術を採用することができる．

対称鍵暗号化：対称鍵暗号化では，暗号化と復号のために 1 つの鍵のみが使用される．非対称鍵暗号化よりも高速に暗号化を行うことができるが，被害者が鍵を入手してファイルを復号することができる可能性がある．例えば，PayBreak [16] は，暗号化機能を提供する Windows API の関数をフックして暗号化に使用される共通鍵を取得することで復号を可能にしている．そのため攻撃者は，鍵が被害者からアクセスできないようにする必要がある．**図 2.2** より，ランサムウェアが採用する対称鍵暗号化アルゴリズムとしては AES が最も人気であることがわかる．

非対称鍵暗号化：非対称鍵暗号化では，暗号化鍵 (公開鍵) と復号鍵 (秘密鍵) の 2 つの鍵が使用される．被害者が公開鍵を入手しても暗号化されたデータを復号することはできないため，対称鍵暗号化に比べて暗号化速度は劣るが，暗号化鍵の保護を行う必要がない．常に同一の鍵ペアを使用する場合，一度秘密鍵が漏洩 (または，ある被害者が身代金を支払って秘密鍵を取

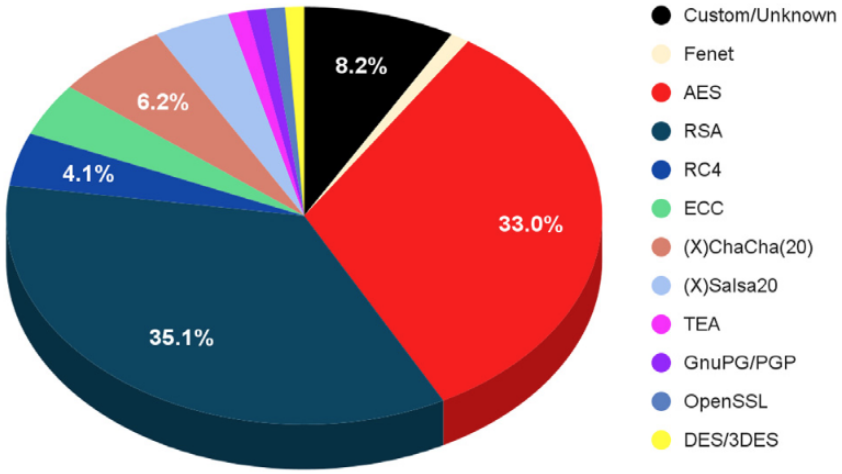

図 2.2. Breakdown of encryption algorithms used by major ransomware families (1989–2021). [2]

得) すると，その鍵ペアで暗号化されたデータは全て解読可能となる．そのため CryptoLocker [17] などの一部のランサムウェアは，被害者ごとに異なる鍵ペアを生成する戦略を採用している．RSA が最も頻繁に，楕円曲線暗号が次いで使用されていることが**図 2.2** よりわかる．

ハイブリッド暗号化：ハイブリッド暗号化では，対称鍵暗号を用いてデータを暗号化した後，その暗号化鍵を非対称鍵暗号化アルゴリズムを用いて暗号化する．これにより大量のデータの暗号化を効率よく実行しつつ，対称鍵暗号化における問題点であった鍵の保護を解決することができる．近年の著名なランサムウェアはハイブリッド暗号化を採用しているものが非常に多い [2]．代表例としては WannaCry [18] や CTBLocker [8] が挙げられる．

2.2.3 暗号化の対象に基づく分類

ランサムウェアは OS 上でユーザが扱うデータファイル (e.g. .docx, .xlsx, .jpg) を暗号化することが一般的であるが，ファイル以外の単位で暗号化を行うランサムウェアも存在する．Mamba [19] はハードディスク全体を暗号化したのちマスターブートレコード (MBR) を書き換えて OS の正常な起動を阻害し，OS 起動時にランサムノートが表示されるようにする．また，Petya [19] は Windows システムのマスターファイルテーブル (MFT) [*1]を暗号化することでファイルのアクセスを不可能にする．DarkSide [20] は VMWare ESXi [21] のホストマシン上で実行される．DarkSide は実行中の仮想マシン (VM) を強制終了させ，VM の仮想ディスクなどの関連ファイルを暗号化する．これらのファイルは，典型的には`/vmfs/volumes`ディレクトリ以下のファイルであるが，仮想マシンからは認識できない．

今日のクラウドサービスの隆盛に伴い，クラウド環境を対象としたランサムウェア攻撃が

[*1] MFT は Windows システム内に存在するファイルの物理的な位置，ファイル名，作成者などのメタデータを管理するデータ構造である．

増加している．ALIBABA Cloud の仮想ストレージサービスは 2023 年の第三四半期のみで 1000 件以上の被害報告をユーザから受けており，2021 年と比較して 118% の増加率を示している [22]．さらに Zscaler 社 は，クラウドサービスやクラウド上のワークフローに最適化されたランサムウェアが開発されることを予測 [23] しており，新しいタイプのランサムウェアの出現に備える必要がある．

2.3　ランサムウェアの影響

2.3.1　発生する影響の種類

ランサムウェア攻撃を受けた組織には，以下のような影響が発生する可能性がある．

データ損失：ランサムウェアによってデータが利用不可能になった場合，攻撃者に身代金を支払ったとしてもデータが復旧される保証がない．SpyCloud 社のレポート [3] (**図 2.3**) によると，2024 年にランサムウェア攻撃者に対して身代金を支払った組織のうち，暗号化されたデータを完全に復旧することができたのは約 50% である．バックアップを定期的に取得していたとしても，最新のバックアップからランサムウェア攻撃が発生するまでの間に更新されたデータは失われる [22].

金銭的損失：攻撃者に支払う身代金がコストとして発生する．さらに，システムダウンやデータアクセスの制限により，業務が停止することで本来のサービスが提供できなくなるためサービスのダウンタイム中に機会損失が発生するほか，復旧作業の費用 (データ復旧，セキュリティ対策や調査の人件費，デバイスやネットワークの修理費用など) も生じる．

信頼性の低下：ランサムウェア攻撃を受けた組織は，データの保護やセキュリティへの投資が不十分であるとの印象を顧客や取引先に与えることがある．これにより既存の顧客や取引先との取引関係が損なわれる可能性があり，またメディア報道によってネガティブなイメージが喧伝されるおそれもある．

長期的なリスク：CyberReason 社の調査 [24] によると，ランサムウェア攻撃を受けて身代金を支払った企業は，その 8 割が再度ランサムウェア攻撃を受ける．したがって身代金支払いによって一度の攻撃に対処したとしても，その後も計測的に攻撃の対象となるリスクがある．

2.3.2　ランサムウェア被害の統計

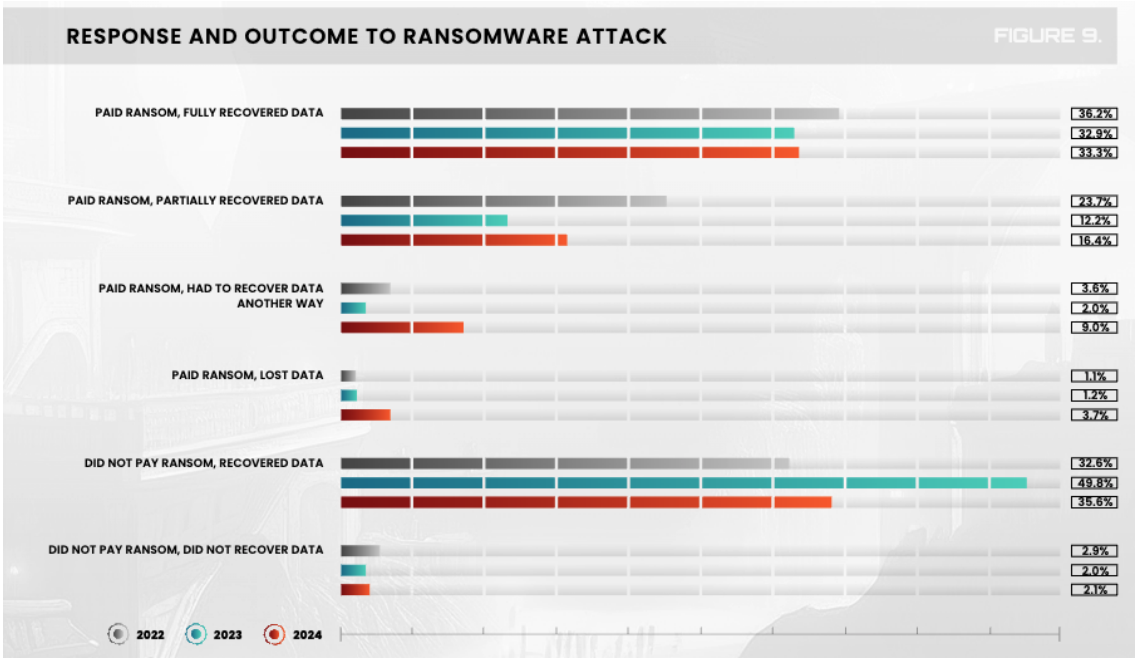

図 2.3. This figure illustrates the outcomes of ransomware attacks based on whether victims paid the ransom and the success rate of data recovery. It categorizes results into fully recovered data, partially recovered data, recovery through alternative means, lost data despite paying, and outcomes for those who did not pay. The percentages are shown for the years 2022, 2023, and 2024. [3]

第 3 章

結論

これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．

これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．

これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．

これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．

これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．これは，結論の文章である．

発表文献と研究活動

(1) 手塚尚哉, 宮本大輔, 明石邦夫, 落合 秀也, ”ファイルの侵害をフックすることによるランサムウェアからのデータ保護システム”. CSS2024, https://conferenceservice.jp/registration/css2024/mypage/proceedings/IPSJCSS-2024150.pdf, 2024.10.24.

参考文献

[1] Gourav Nagar. The evolution of ransomware: Tactics, techniques, and mitigation strategies. *Valley International Journal Digital Library*, pp. 1282–1298, 2024.

[2] Kenan Begovic, Abdulaziz Al-Ali, and Qutaibah Malluhi. Cryptographic ransomware encryption detection: Survey. *Computers & Security*, Vol. 132, p. 103349, 2023.

[3] SpyCloud. 2024 malware & ransomware defense report — spycloud. `https://spycloud.com/resource/2024-malware-ransomware-defense-report/`. (Accessed on 12/09/2024).

[4] Harun Oz, Ahmet Aris, Albert Levi, and A Selcuk Uluagac. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, Vol. 54, No. 11s, pp. 1–37, 2022.

[5] Virus Bulletin. Trojan horse: Aids information introductory diskette version 2.0. `https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf`. (Accessed on 12/08/2024).

[6] Wikipedia. Pgpcoder - wikipedia. `https://en.wikipedia.org/wiki/PGPCoder`. (Accessed on 12/08/2024).

[7] Mingcan Cen, Frank Jiang, Xingsheng Qin, Qinghong Jiang, and Robin Doss. Ransomware early detection: A survey. *Computer Networks*, Vol. 239, p. 110138, 2024.

[8] SOPHOS. The current state of ransomware: Ctb-locker – sophos news. `https://news.sophos.com/en-us/2015/12/31/the-current-state-of-ransomware-ctb-locker/`, 2015. (Accessed on 12/08/2024).

[9] Dermot Byrne and Christina Thorpe. Jigsaw: an investigation and countermeasure for ransomware attacks. In *European Conference on Cyber Warfare and Security*, pp. 656–665. Academic Conferences International Limited, 2017.

[10] Jian Huang, Jun Xu, Xinyu Xing, Peng Liu, and Moinuddin K Qureshi. Flashguard: Leveraging intrinsic flash properties to defend against encryption ransomware. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pp. 2231–2244, 2017.

[11] Cloudflare. What are petya and notpetya? — ransomware attacks

— cloudflare. https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/. (Accessed on 11/22/2024).

[12] SOPHOS. 2024 ransomware report: Sophos state of ransomware. https://www.sophos.com/en-us/content/state-of-ransomware. (Accessed on 11/21/2024).

[13] 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 11/23/2024).

[14] ISO. Iso/iec 27001:2022 - information security management systems. https://www.iso.org/standard/27001, 2022. (Accessed on 12/09/2024).

[15] Pranshu Bajpai, Aditya K Sood, and Richard Enbody. A key-management-based taxonomy for ransomware. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12. IEEE, 2018.

[16] Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele. Paybreak: Defense against cryptographic ransomware. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, pp. 599–611, 2017.

[17] Kevin Liao, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin. In *2016 APWG symposium on electronic crime research (eCrime)*, pp. 1–13. IEEE, 2016.

[18] Maxat Akbanov, Vassilios G Vassilakis, Ioannis D Moscholios, and Michael D Logothetis. Static and dynamic analysis of wannacry ransomware. In *Proc. IEICE Inform. and Commun. Technol. Forum ICTF 2018*, 2018.

[19] Qublai K Ali Mirza, Martin Brown, Oliver Halling, Louie Shand, and Abu Alam. Ransomware analysis using cyber kill chain. In *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 58–65. IEEE, 2021.

[20] TrendMicro. Darkside on linux: Virtual machines targeted — trend micro (us). https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html, May 2021. (Accessed on 12/09/2024).

[21] vmware. Vmware vsphere — virtualization platform. https://www.vmware.com/products/cloud-infrastructure/vsphere. (Accessed on 12/09/2024).

[22] Zhongyu Wang, Yaheng Song, Erci Xu, Haonan Wu, Guangxun Tong, Shizhuo Sun, Haoran Li, Jincheng Liu, Lijun Ding, Rong Liu, et al. Ransom access memories: Achieving practical ransomware protection in cloud with {DeftPunk}. In *18th USENIX Symposium on Operating Systems Design and Implementation (OSDI 24)*, pp. 687–702, 2024.

[23] Zscaler. 2023 threatlabz state of ransomware report — zscaler. https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report, 2023. (Accessed on 12/09/2024).

[24] CyberReason. Ransomware: True cost to business 2024. https://www.cybereason.com/blog/ransomware-true-cost-to-business-2024. (Accessed on 12/09/2024).

謝辞

ありがとうございました！

付録 A

ソースコード

```
int main () {
  ...
  ...
}
```