一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

LockBit3.0 ウェブサイトのデータ変遷に基づく 攻撃者と被害者の行動の分析

関根　悠司* 　Yin Minn Pa Pa† 　吉岡　克成†,‡ 　松本　勉†,‡

∗ 横浜国立大学大学院環境情報学府
† 横浜国立大学先端科学高等研究院
‡ 横浜国立大学大学院環境情報研究院

あらまし　LockBit3.0 は 2022 年 7 月から活動しているランサムウェアグループの 1 つであり，被害企業は 2023 年 6 月までの累計で 1,000 件を超えている．2024 年 2 月には国際的な法執行活動 Operation Cronos により関係するサーバのテイクダウン，暗号通貨アカウントの凍結等が行われ，関係者が逮捕されているが，本研究報告の執筆時点ではその詳細は明らかになっていない．LockBit3.0 はランサムウェアの被害者情報や漏えいデータをダークウェブ上で公開・暴露すると共に，第三者への漏えいデータの販売や RaaS（Ransomware as a Service）等のビジネスモデルを構築している．公開される情報は被害者との交渉結果を反映していると推測されるが，その時間的変化や，交渉内容，支払い，支払い期限の延長といった行動との関係性の分析は十分に行われていない．本研究では LockBit3.0 のサイトに掲載される被害者情報や身代金額の時間的変化を 166 日間に渡り継続的に監視し，掲載情報の変化と，その変化が攻撃者と被害者の行動とどのように関連しているかを分析した結果を報告する．
キーワード　ランサムウェア，マルウェア，スレットインテリジェンス，LockBit

Analyzing Attackers and Victims Actions via LockBit3.0 Website Data Dynamics

Yuji SEKINE*, Yin MINN PA PA†, Katsunari YOSHIOKA†,‡, and Tsutomu MATSUMOTO†,‡

∗ Graduate School of Environment and Information Sciences, Yokohama National University
† Institute of Advanced Sciences, Yokohama National University
‡ Faculty of Environment and Information Sciences, Yokohama National University

Abstract　LockBit3.0 is one of the top ransomware groups that has been active since July 2022, targeting over 1,000 companies. In February 2024, Operation Cronos, an international law enforcement operation, took down the servers involved, froze the cryptocurrency accounts, and arrested the people involved, but at the time of writing this research report, the details of the operation are not yet known. LockBit3.0 operates as a RaaS (Ransomware as a Service) model, expose victim information and leaked data on their darkweb website while selling the leaked data to the third parties. The information exposed on their website may change according to the victim's negotiation. However, how these changes are related to the victims' actions such as negotiation, extension of ransomware payment deadline has not been well studied. In this study, we monitor LockBit3.0 website over a 166-days period to analyze how the changes of victim information and ransomware payment deadline relate to the actions of attackers and victims.
Key words　Ransomware,Malware,Threat Intelligence, LockBit

1. ま え が き

組織の情報システムに侵入し重要データを暗号化したり盗み出した上で，そのデータを復元・廃棄する対価として身代金を要求するランサムウェアによる攻撃が大きな問題となっている．

警察庁が公表している日本の企業・団体におけるランサムウェアの被害数は 2020 年下半期以降年々増加しており，2022 年に 230 件に達している [1]．ランサムウェアの開発や攻撃を行っているランサムウェアグループのひとつである LockBit は，2020 年 1 月頃に活動を開始し，2022 年 7 月頃から LockBit3.0

という形態で活動している [2]．なお，2024 年 2 月に国際的な法執行活動 Operation Cronos [3] により関係するサーバのテイクダウン，暗号通貨アカウントの凍結等が行われ，関係者が逮捕されているが，本研究報告の執筆時点ではその詳細は明らかになっていない．

LockBit3.0 は，RaaS（Ransomware as a Service）のビジネスモデルで運営されている．RaaS は，ランサムウェアグループが作成したランサムウェアを他の攻撃者に提供するサービスであり，LockBit3.0 ではランサムウェアそのものの提供だけでなく，交渉するためのプラットフォーム（チャットスペース等）も提供している．身代金の受取りは，仮想通貨で行われ，その内の一定の割合（LockBit3.0 では 20%）をサービス提供者に支払う形になっている．RaaS の提供者である LockBit3.0 と利用者である個々の攻撃者の活動を明確に区別することは困難であるため，本報告では両者を含めて攻撃者と呼ぶ．LockBit3.0 のウェブサイトは，ダークウェブ上でホスティングされ，被害者の組織情報，漏えいデータのサンプルの提示，漏えいデータの販売，交渉チャットログの公開など被害者に関わる情報を広範囲に公開している．ランサムウェアの被害者は，チャットを通じて交渉したり，ウェブサイトを通じて支払いを行ったり，支払い期限を延長したりすることができる．また，第三者はウェブサイトを通じてデータを購入したり，データを削除することができる．

世界の企業・団体の LockBit3.0 の被害数は活動開始から 2023 年 6 月初旬まで 1,000 社を超えている [4]．前述の通り，LockBit3.0 は被害者に関するいくつかの情報をダークウェブ上のサイトで公開し，被害者のデータを販売しており，サイト上で公開される情報は被害者との交渉や支払いの状況によって変更される．そのため，これらの変化を分析することで，攻撃グループと被害者の活動や交渉の状況を推定できる可能性がある．しかし，公開されている情報が時間と共にどのように変化するかはこれまで詳細に分析されておらず，その変化が交渉・支払い・期限延長といった行動とどのように関連しているのかも明確になっていない．そこで本研究では LockBit3.0 のサイトに掲載される被害者情報や身代金額，情報開示までの猶予時間等の時間的変化や攻撃グループと被害者の間で行われたチャット履歴を調査することで，その背景にある交渉や LockBit3.0 の活動の状況を推定することを試みた．2023 年 6 月 27 日から 12 月 10 日までの 166 日間，LockBit3.0 のサイトに 6 時間に一度（観測開始から最初の 1 週間は 1 時間に一度）アクセスし，掲載情報を収集・蓄積し，その変化を分析した．さらに，交渉内容のチャット履歴が暴露されている 41 件についてその内容を分析した．

分析の結果は以下の通りである．まず LockBit3.0 サイトから 166 日間の観測期間中に合計 1,348 件の被害者情報が得られた．このうち，観測開始時から既に漏えいデータが公開されている状態，すなわち，交渉に応じなかったり，交渉が決裂したことで情報が暴露された状態が続いている被害者が 884 件（65.6%）確認された．サイトに掲示されている被害者の多くがこの状態であり，交渉に応じないことで見せしめとして長期間サイト上に晒されている状況が推察される．一方，観測期間中に漏えいデータの公開期限のカウントダウンが行われていた被害者は 464 件（34.4%）であり，そのうち，突然サイト上で当該被害者の掲載が無くなったケース，すなわち，身代金を支払った可能性のあるものは 71 件（15.3%）であった．また，漏えい情報の公開期限延長の費用を支払った可能性のあるものは 36 件（7.8%）であった．また，平均の期限延長時間は 8.2 日，最長の延長時間は 56.3 日であった．

LockBit3.0 サイトおよび暴露されたチャットにおいて確認された身代金額は，平均で 453 万米ドル（約 6.6 億円）であり，最小で 10 万米ドル（約 1,500 万円），最高で 8,000 万米ドル（約 116 億円）であった．全被害者 1,348 件のうち，漏えいデータの購入価格等がサイトに表示され，サイト上で任意の訪問者による漏えいデータの購入が可能と推定されるケースが 275 件（20.0%）あり，第三者に情報が漏えいするリスクを生じさせることで被害者に強い圧力を与える状態となっていた．一方，サイト上での漏えいデータの購入が可能な場合とそうでない場合で購入可能な場合の身代金金額の方が低かった．暴露されたチャットのやり取りの主な内容は，漏えいデータの確認や身代金額の交渉だった．これらの交渉において被害者の代理で交渉を行う代理人の明確な存在が 41 件のチャット中 2 件で確認された．第三者が購入可能な漏えいデータの一部はダウンロードが可能な状態となっており，それらは 36 のクリアウェブのドメインと 33 のダークウェブのドメインにホスティングされていた．

上記のように，攻撃者と被害者の間のやりとりや身代金の支払いの実態の一部が明らかとなったが，これらの結果は，サイト上で公開されている情報を基にしており，実際の交渉や支払いの多くはサイトに被害者情報が掲載される以前に行われている点に注意が必要である．

2. 関 連 研 究

Gazet [5] は 14 のランサムウェアを静的解析し，コードの品質，マルウェアの機能，暗号プリミティブの分析を行い，ランサムウェアに関係するビジネスモデルやランサムウェアを取り巻くコミュニケーションの分析の足掛かりとなる技術的な検証を行ったが，発表から 10 年以上経っているため，現在のランサムウェアのビジネスモデルやコミュニケーションは大きく変わっている．また，文献 [5] の研究手法はランサムウェアを解析し，検証を行っているが，本研究の手法は，ランサムウェアそのものではなく，ダークウェブ上のランサムウェアグループサイトの掲載情報に基づき，グループの行動を分析している．Symantec のレポート [6] では，Symantec が確認している 16 のランサムウェアについて分析し，仕分けたランサムウェアファミリーの調査結果と，ランサムウェアグループの資金の入手方法や，ランサムウェアの脅威について論じている．しかし，このランサムウェアファミリーやランサムウェアには LockBit ファミリーや LockBit3.0 は含まれておらず，近年最も活発な活動をしている LockBit3.0 の資金入手方法は明らかになっていない．Khan [7] は LockBit のランサムウェアを検出し防御する方法を調査しているが，漏えいデータの扱いやそれらの公開，被害者

との交渉に関する言及はない．いくつかのオンライン記事 [8]〜[10] では，入手した LockBit3.0 の検体をもとにランサムウェア自体の仕組みを調査している．具体的には，ファイル暗号化の特徴や，他のランサムウェアとの類似点など，ソフトウェアの観点からランサムウェアの動作を分析している．しかし，これらの記事では，ランサムウェアを作成している組織や，それを利用しているアフィリエイトがどのように活動をしているかに関しては，明らかにしていない．

Akinyemi ら [11] も前述の Web 記事と同様にランサムウェア自体に注目し，LockBit3.0 が LockBit や LockBit2.0 とは異なり，主にソーシャルエンジニアリングを用いて被害者のネットワークに侵入していることを明らかにしている．また，Meurs ら [12] はランサムウェアの被害者が身代金を支払いやその金額を決定する要因として保険加入の有無，盗み出されたデータの内容，被害組織の収益が関連していることを明らかにした．これらの研究では盗取したデータの扱いや被害者との交渉内容については分析されていない．本研究では，二重脅迫型のランサムウェアにおいて被害者情報が公開される点に着目し，攻撃グループのサイトに掲載される情報の時間的変化から交渉の状況を分析する．

3. LockBit3.0

3.1 LockBit3.0 のビジネスモデル

一般にランサムウェアによる攻撃では，攻撃者は組織の情報システムに侵入し内部のデータを暗号化したり盗み出し，そのデータの復元や廃棄する対価として被害者に身代金（ransom）を要求する．LockBit3.0 は被害組織に関する情報や漏えいデータを開示するためのホームページをダークウェブ上に有しており，当該ページの存在はマスメディアを含めて広く知られていることから，掲載された情報やデータは事実上公知の状態となる．特に LockBit3.0 はホームページにおいて漏えいデータの販売をおこなっており，被害者以外の第三者も販売対象となる場合がある．RaaS として活動している LockBit3.0 では，組織への侵入や情報の盗取，被害者との交渉や情報の公開，身代金の受け取りといった一連のプロセスは分業化が進んでいる．LockBit3.0 は組織に侵入して情報を盗取する攻撃者のアフィリエイトとしても機能しており，アフィリエイト募集のページでは，アフィリエイト参加者は LockBit3.0 が用意する管理パネルで提供されているツールを利用して攻撃を容易に行うことができるが，身代金の 20% を LockBit3.0 に収める必要があると記載されている．また，特定の国々や重要インフラへの攻撃を禁止している．

3.2 LockBit3.0 サイト

前述の通り，LockBit3.0 はダークウェブ上に情報公開用のサイトを有しており，当該サイトには被害者の情報が載っている（図 1）．各被害者の情報はブロック単位で表示され，全被害者分のブロックは 1 つの Web ページ（ホームページ）にまとめられている．具体的には被害組織のドメインまたは社名・団体名，被害組織の説明文，盗み出したデータの概要，更新日といった情報がホームページに掲載される．ブロックは三種類あり，カウントダウンタイマーと金額タグのあるもの，カウントダウンタイマーだけのもの，カウントダウンタイマーも金額タグもないものに分かれる．この内，前 2 つは赤のブロックで，最後の 1 つは緑のブロックで表現されている．ホームページ上の企業のブロックをクリックすることで当該組織のロゴマーク，盗み出したデータの一部のスクリーンショットが閲覧できる．各被害組織には情報開示までのタイムリミットが与えられており，これが残っている間は当該ページにおいてカウントダウンが行われる．既にタイムリミットを過ぎている場合にはカウントダウンは表示されず，代わりに漏えいデータのリンクが表示され，漏えいデータは公開状態となる．また，カウントダウンの有無とは別に，被害組織によっては，「タイムリミットを 24 時間延長する」「全てのデータを破壊する」「全データをダウンロードする」という 3 つのボタン（図 2）が用意され，それぞれのアクションに対する金額が提示される．さらに，一部の被害組織については，攻撃者と被害者との交渉の経緯を示すチャット履歴も公開されている．

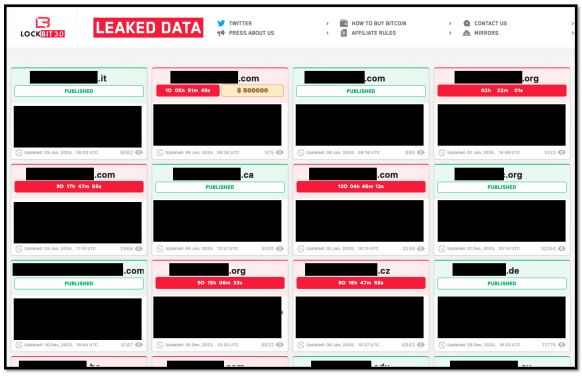

図 1　LockBit3.0 のホームページ

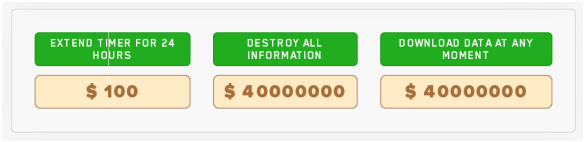

図 2　漏えいデータに対するアクションとその金額の例

ランサムウェアグループの多くは複数のドメイン（ミラーサイト）を有しており，LockBit3.0 は少なくとも 2023 年 12 月 10 日時点で 9 個のミラーサイトを運用していることが，LockBit3.0 のサイトから確認できる．これらのサイトでは自動化された情報収集や DoS 攻撃への対策が施されている場合が多く，LockBit3.0 ホームページにアクセスすると，DoS 対策として，7 秒間程度ミラーサイトのリンクが載ったページが表示された後，ホームページが表示されるようになっている．

4. LockBit3.0 サイトのスクレイピング

3.2 節で示した LockBit3.0 のサイトに定期的にアクセスし情報を収集する仕組みを実装し，2023 年 6 月 27 日 12 時から 2023 年 12 月 10 日 21 時までの計 166 日と 9 時間に渡り観測を行った．情報収集を開始した 6 月 27 日から 7 月 3 日 9 時までは 1 時間に 1 度アクセスを行ったが 1 時間単位では収集される

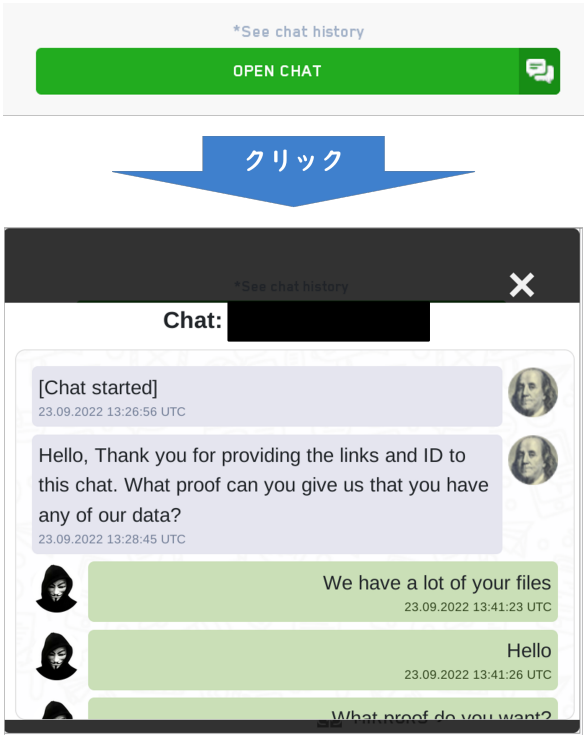

図 3　チャット履歴の表示ボタンと表示されるチャット

情報の変化が小さかったため，それ以降は 6 時間に 1 回収集を行った．観測に失敗した期間は累計で 35 日間あり，これらの大部分はダークウエブにアクセスするためのアプリケーションである torproxy [13] が起動しておらずスクレイピングできなかったことが原因だった．また，2023 年 12 月 1 日頃に LockBit3.0 側でホームページのマイナーチェンジを行ったため，その後 3 日分はデータの蓄積に失敗した．前述の通り，一部の被害組織については攻撃者と被害者とのチャット履歴が公開されている（図 3）ため，2023 年 9 月 17 日時点で LockBit3.0 サイトに掲載されていた被害組織別のページに前述と同様のスクレイピング手法を用いてアクセスし，チャット履歴を取得した．

スクレイピングには Selenium [14] を用いた．その際，ダークウェブにアクセスするためのアプリケーションとして dperson/torproxy [13] を使用した．スクレイピングにより得た HTML ソースは，python ライブラリである BeautifulSoup4 [15] を用いて整形しデータベースに保存した．データベースに保存した情報は，被害組織のドメイン名，漏えいデータの説明および被害組織の説明文，データ公開までのカウントダウン，提示価格，被害者ごとのページの更新日時，閲覧数および URL である．

5. 調 査 結 果

5.1 節では観測期間中の各被害者の公開状態の変化を分析し，その変化が示唆する攻撃者や被害者の行動の内容を考察する．5.2 節では第三者へのデータ販売が行われている場合に，これらのデータがホスティングされている環境を調べることで，LockBit3.0 の使用するインフラを分析する．5.3 節では，LockBit3.0 サイトで公開されているチャット履歴を分析し，交渉内容や身代金額，チャットによる交渉とサイトにおける被害者情報の公開状況の関連性を分析する．

5.1 被害者情報の公開状態の分析

前述の通り LockBit3.0 のサイトに掲載される被害者情報にはいくつかの状態があるが，漏えいデータ公開までのカウントダウン表示の有無という観点で区別できる．カウントダウンの表示は情報開示の期限が迫っており，被害者は交渉によりこれを中止させるかの判断を迫られている状態であることを示唆し，逆にカウントダウン表示がないことは，既に何らかの情報や漏えいデータが開示されている状態であることを示唆する．

観測期間中にサイトにて観測された被害者の総数は 1,348 件であった．観測期間中 1 度でも情報開示までのタイムリミットがカウントダウンされていた被害者数は 464 件であった．

図 4 は，観測結果を時系列で可視化したものである．縦軸は被害者，横軸は時間を示している．観測システムの運用上の問題でそもそもスクレイピングができなかった期間は黒く塗りつぶしている．スクレイピングが成功した期間について各被害者に対するカウントダウンの有無によって色を変えて表示した．まず，カウントダウンが表示されている場合は赤，カウントダウンが表示されていない場合は緑とし，ホームページに当該被害者の情報が全く掲載されていない場合は着色なし（空白）とした．大きく上下に分けているのは漏えいデータに対する金額タグの有無で，上側は金額タグあり，下側は金額タグなしである．

支払いが示唆されるケース 攻撃グループとの交渉の状況を分析する上で最も注目すべきは，カウントダウン状態（赤）からの変化である．カウントダウン中に非掲載状態（空白）に遷移した場合は，身代金の支払いに応じたためサイトでの被害者情報が削除されたことが推測される．カウントダウン状態を含む被害者の状態変化を図 5 に示す．カウントダウンから掲載終了への状態遷移は上側は 14 件，下側は 68 件の計 71 件が確認され，カウントダウンが表示された全被害者 464 件の少なくとも 15.3% で支払いが行われたと推定されることが分かった．

図 6 は支払いを行ったと推定される事例における漏えいデータ公開までの残り時間の分布である．縦軸は被害者数，横軸は非掲載になったときに残っていたカウントダウンの日数を示す．この図から，公開までの残り時間が 5 日以内で身代金を支払った被害者が多いことがわかる．残りが 10 日よりも多かった 6 件の内，5 件は 10 日から 14 日の間であったが，残り 1 件は 34 日間残した状態で非掲載になっていた．

支払いに応じず漏えいデータが公開されるケース カウントダウンが終了するまでに情報公開中止等の交渉が成功しないと，漏えいデータが公開される．観測期間中にカウントダウンが行われ（赤），その後，漏えいデータが公開状態となったケース（緑），すなわち，支払いに応じなかったことが示唆されるケースは，合計 370 件あった．また，観測開始時点で既に公開状態（緑）となっている被害者が 789 件あった．これらは攻撃グループとの交渉に応じず，または，交渉決裂により漏えいデータが公開された被害者が時間経過と共に蓄積された結果であると推定され，このような状態の被害者が多数存在することは，一度公開状態となると長期間に渡りその状態が続くことを示唆している．一方，351 件の被害者については公開状態（緑）から非

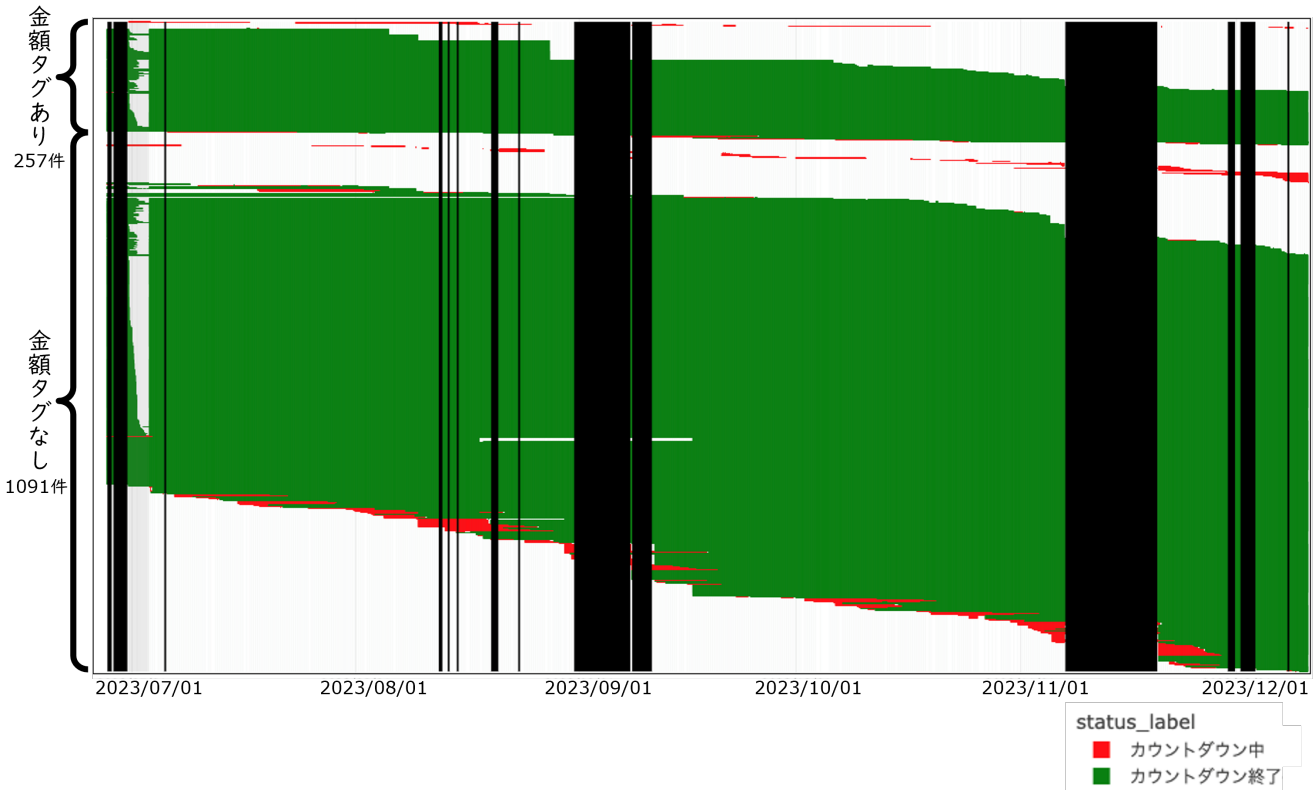

図 4　被害者情報の公開状態の時間変化

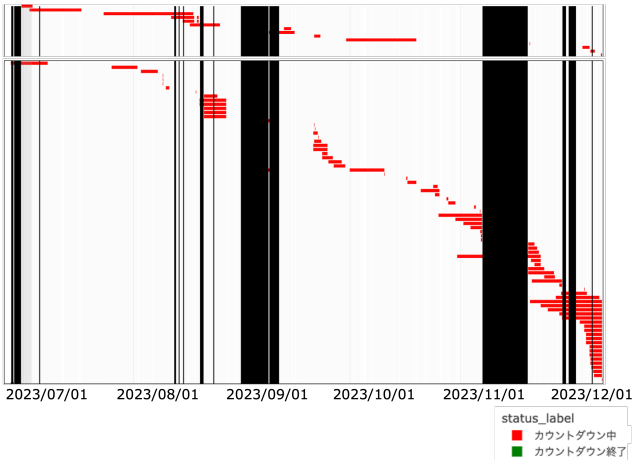

図 5　支払いが示唆されるケース（カウントダウン中の掲載中止）

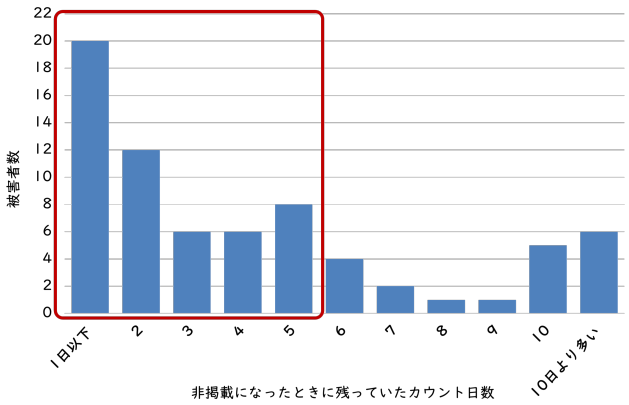

図 6　支払いが示唆される被害者の残り時間

掲載状態（空白）へと変化し，ホームページでの公開が終了していることが分かるが，この変化の理由が被害者の継続的な交渉による結果であるか，攻撃グループ側の判断による掲載終了であるかは定かではない．

第三者へのデータ販売 前述の通り，LockBit3.0 では，被害者だけでなく，第三者にもデータの販売を行う場合がある．図 4 の概観通り，金額を提示して第三者のデータ購入等を可能にしているケース（上側：257 件）は第三者による介入ができないケース（下側：1091 件）に比べて少なく，実際には LockBit3.0 サイトに掲載されない被害者も多数存在することを勘案すると，第三者へのサイト上でのデータ販売は限定的であり，被害者との直接交渉が主流であると推定される．LockBit3.0 のホームページで掲載されている金額は購入するための金額であり，緑のブロックで掲載されている被害者でもホームページのソースを確認するとその金額を確認することができる．この購入するための金額は平均で約 82 万米ドル（約 1.2 億円），最小で 1.4 万米ドル（約 210 万円），最大で 4 千万米ドル（約 60 億円）である．

情報公開期限の延長 前述の分析に加えて，カウントダウン時の情報公開期限までの残り時間の変化を分析した結果を表 1 に示す．観測期間中に情報公開期限の延長があった被害者は 38 件，変更回数の総計は 57 回あり，期限の延長も行われていることがわかった．1 被害者あたりの最大の変更回数は 3 回で，最大の変更時間は 56 日と 7 時間 20 分の延長であった．1 か月以上の延長は 4 回あった．また，延長ではなく短縮された被害者も 4 件あり，最短 40 分，最長約 10 日 4 時間の短縮がされていた．

表 1　情報公開期限の延長回数（～の左側の数値は含まない）

延長時間	回数
0 秒未満（期限短縮）	4
0 秒～12 時間	11
12 時間～1 日	1
1 日～3 日	13
3 日～1 週間	10
1 週間～2 週間	7
2 週間～1 か月	7
1 か月～	4

LockBit3.0 サイト上では 24 時間単位の延長のための金額が提示されているが（図 2），24 時間単位で延長されることはほとんどなく，延長は個別の交渉で行われている可能性がある．個別の交渉については 5.3 節のチャット履歴の分析で説明する．

5.2　サンプルデータのホスティング状態の分析

漏えいデータ公開後も金額が提示されるケース（図 4 の上側の緑）においては，前述の通り，被害者ごとのページに図 2 のようにデータを購入したり廃棄するアクションを選ぶボタン（金額タグ）が表示されるが，これとは別に無料で何らかのデータをダウンロードできるボタンが表示される場合がある．2023 年 12 月 3 日 16 時頃に調査したところ，この時点で金額が提示されて公開状態であった 106 件のうち 70 件にダウンロードボタンが存在した．これは提示金額を支払うことで得られる漏えいデータの一部，すなわちサンプルデータであると推定される．

ダウンロードボタンのリンクを調べると，ダークウェブの URL が 34 件，クリアウェブの URL が 36 件確認された． ダークウェブの URL34 件のうち LockBit3.0 のサイトと同じドメインが 21 件，LockBit3.0 のアーカイブサイトのドメインが 1 件，LockBit3.0 以外のダークウェブドメインが 12 件だった． クリアウェブの URL36 件からは 13 個のドメインを得られ，その内ファイル共有サービスのドメインが 5 件，既存会社と関係のないドメインが 5 件，セキュリティ会社が 1 件，衣服のショッピングサイトが 1 件，テレビとパソコンの修正サービス会社が 1 件だった．セキュリティ会社，衣服のショッピングサイト，テレビとパソコンの修正サービスのドメインに関しては正規サービスに何かの脆弱性があり，攻撃者に悪用された可能性がある．このように攻撃者は漏えいデータのサンプルを多様なネットワークリソースを活用してホスティングしている実態が明らかになった．

5.3　公開されたチャット履歴の分析

2023 年 9 月 17 日時点で攻撃者との交渉内容であるチャット履歴が公開されていた被害者の数は 41 件であり，これらのすべての履歴の収集に成功した．メッセージ数の合計は 1,886 件で，メッセージ数は最大 237 件であった．以下ではその内容を分析した結果を示す．

チャットメッセージ数とチャット継続期間 41 件のチャット履歴を構成するメッセージ数とチャット継続期間を図 7 に示す．図 7 は縦軸がメッセージ数，横軸がチャット継続時間である．この図から多くの被害者の交渉期間は 50 日以下でメッセージ数は 100 件以下であることがわかる．特徴的なケースとしてケース A から D が確認された．ケース A では，1 か月以内に 200 件を超えるメッセージのやり取りが行われ，その中では身代金の一部の支払いが示唆される内容も含まれていた．ケース B では 130 日以上に渡り断続的にやり取りがされていた．ケース C では 2 日間程度交渉が行われたあと，9 か月に及ぶ空白期間があり，その後，被害者側から攻撃側への批判的な発言と共に終了していた．ケース D では，当初 2 か月程度で交渉が行われ，半年程度の空白期間の後，被害者側からの無意味な文字列の投稿と共にチャットが終了していた．

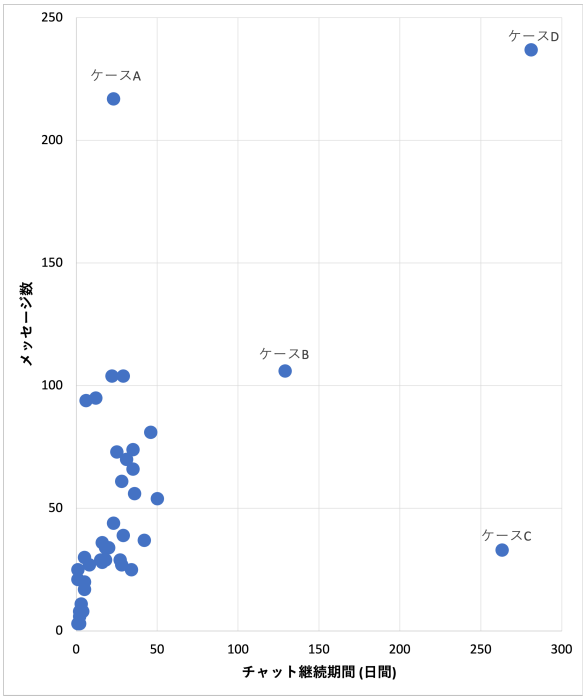

図 7　チャット履歴に残っていたメッセージ数とチャット継続期間

チャット内の金額交渉 大部分のチャットで金額交渉が行われており，2 件では仲介者を通した交渉が確認された．身代金金額が提示されているものは 41 件中 29 件あり，金額は 10 万米ドルから 8000 万米ドル（約 1500 万円から約 116 億円）で，平均 453 万米ドル（約 1.5 億円）だった．身代金の要求に対して最大で 100 万米ドル（約 1.5 億円）までの支払いに応じると回答した被害者があったが，最終的には交渉を拒否していた．交渉時には，被害者側は情報漏えいの事実の確認のため，漏えいデータのファイルリストの提示を要求し，漏えいファイルの内容の確認を希望する場合が多かった．また，LockBit3.0 サイトでの被害者情報の公開を恐れ，漏えいデータの内容に応じて金額の交渉を行おうとする様子が伺えた．これに対して攻撃者側は漏えいファイルの一部を開示し，実際に情報漏えいが発生していることを示すと共に身代金の一定の減額に応じる場合もあった．交渉の結末としては，交渉が失敗していたり，被害者からの応答が途切れたり，被害者が怒りの表現を示すなど交渉が決裂して終わるものが多かったが，これは交渉決裂により公開されたチャット履歴の特徴と言える．

身代金額と第三者へのデータ販売の関係性 図 8 はチャットデー

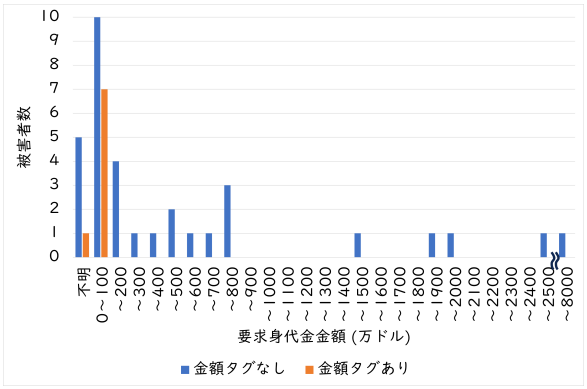

図 8　チャット履歴が公開されている被害者の 1000 万米ドル以下の身代金

タが取得できた 41 件それぞれの身代金の分析である．図 8 では，LockBit3.0 サイトでの公開時に身代金金額が公開されない場合（金額タグなし）と，身代金金額が公開され，第三者でも購入が可能な場合（金額タグあり）に分けて表示している．金額タグありの場合は金額タグなしよりも要求額が低くなっており，第三者でも購入が可能な状況で被害者情報を公開する場合は，比較的身代金金額が低いことが分かる．なお身代金金額が 1000 万米ドルを超えた被害者は 3 件あり，それぞれ 1500 万，2500 万，8000 万米ドルであったが，これらはいずれも金額タグは提示されておらず，高額の身代金を要求する場合は，サイト上での第三者への販売は行っていないことがわかる．

攻撃者が支払いを要求する際に利用した仮想通貨アドレス 身代金の支払いには BitCoin（BTC）が用いられており，チャットには 5 つの BTC アドレスが含まれていた．その内 2 つの BTC アドレスでは入金記録が見つかった．BTC アドレス”bc1qyu...f4afd”の取引を blockchain.com [16] で確認した結果，2024 年 2 月時点では残高ゼロだったが，2022 年 9 月，被害者とのチャット中に 53.10674450 BTC（約 2,757,314 米ドル）が振り込まれていた．当該アドレスについては一件の被害者が 100 万ドルの支払いをした事が関連するチャットの内容から確認された．別の BTC アドレス”bc1qpg...qw5zz”の取引について同様に blockchain.com を利用して確認した結果，2024 年 2 月時点では残高ゼロだったが，2022 年 9 月，被害者とのチャット終了後に 10.28258260 BTC（約 534,441 米ドル）が振り込まれていた．振り込まれる前にチャットが終了していたため関連するチャット内容からは被害者からの支払いは確認できなかった．

チャットと LockBit3.0 サイトでの情報公開の関係 図 9 はチャットが公開された被害者 41 件に関して，チャットの発言と LockBit3.0 サイトの情報公開の状況を同一時系列で可視化した図である．この図に示されている件数は 44 件になっているが，これは 3 件の被害者に対してそれぞれ 2 件ずつサイトで情報公開がされていたためである．いずれの被害者についても，チャットが行われた時期は LockBit3.0 サイトでの情報公開よりも前になっていた．一方，観測期間中にカウントダウンが行われており，観測期間中に漏えいデータが公開された（赤から緑に状態遷移があった）被害者が 3 件存在した．これらを被害者 AY,

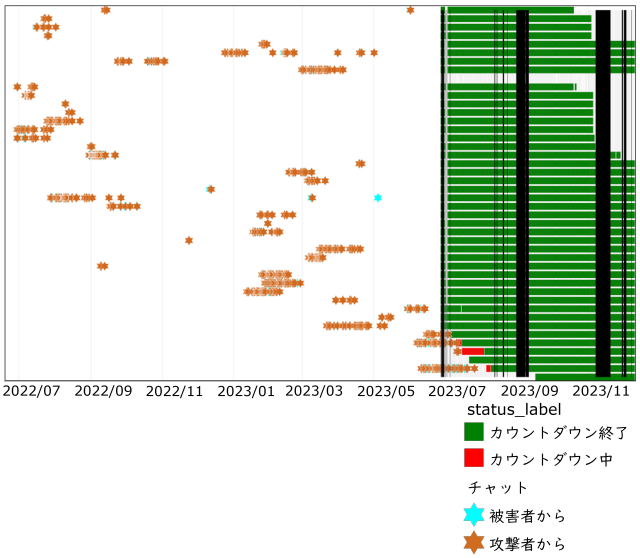

図 9　チャットが確認された被害者の被害者データの状態の時間変化

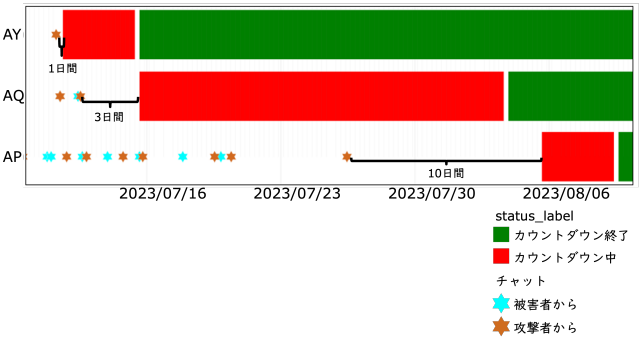

図 10　図 9 のカウントダウン中から終了した（赤から緑）変化がある被害者部分を拡大した図

AQ, AP と呼ぶこととする．図 10 に，この 3 件における時系列を拡大して示す．水色の星が被害者からチャットで発言があった時刻，茶色の星が攻撃者から発言があった時刻を表している．この図から，チャットによる交渉終了後，被害者 AY では約 1 日後，被害者 AQ では約 3 日後，被害者 AP では約 10 日後にサイトに情報が掲載されたことがわかる．これらの被害者以外においても，チャットによる交渉の開始時期は LockBit3.0 サイトの観測実験開始日よりも前であった．このように，チャット等により，まず交渉が行われ，その内容次第でサイトに情報が掲載されるという想定通りの時系列が確認された．被害者がサイトからの情報の削除をチャット上で要求し，これに対応して情報を削除したという攻撃者の発言も 1 件確認されたが，当該チャットは観測時点でも公開されていたことから，その後の交渉の決裂等，何らかの理由により再び掲載されたと推測される．

6. 考　　察

LockBit3.0 サイトにおける公開情報変更と一部のチャット履歴が時間経過と共にどのように変化するかを分析することで，攻撃者と被害者の行動をある程度推定できることがわかった．チャット履歴とサイトの公開情報の時系列分析から，チャットによる攻撃者と被害者の交渉がプライベートに行われ，その交

渉の経緯で被害者情報や漏えいデータのサンプル，そして漏えいデータそのものが公開されていく流れが確認されたが，これは公開情報から確認できる LockBit3.0 の活動が限定的であることを示している．すなわち，チャット等による初期的な交渉が成立し，サイト上には何の情報も掲載されない膨大なケースが存在する可能性がある．

漏えいデータは，LockBit3.0 ホームページのサーバや他のダークウェブ上のサーバだけでなく，クリアウェブのサーバにもホスティングされており，これらの分布は LockBit3.0 とその RaaS サービスを利用する攻撃者の関係を反映している可能性があるが，その裏付けには更なる調査が必要である．また，第三者もデータ購入等が行える状態であるのは，全体の 2 割程度であり，第三者へ金額が明示されていない場合よりも少額の身代金が提示される傾向が明らかになったが，第三者へのデータ販売を行う判断基準や第三者との実際の取引の有無，取引の規模については本観測データからは分析ができなかった．今後，法執行機関によるテイクダウン等により明らかとなる情報が利用できれば，さらに詳細な分析が行える可能性がある．

ランサムウェアによる二重脅迫においては，攻撃者は漏洩情報や被害者の情報を部分的に開示しつつ，交渉を優位に進めようとする．そのため，公開された情報を時間的推移を含めて詳細に分析することで，攻撃者の行動や判断，被害者の対応について多くの情報が得られることがわかった．LockBit3.0 に限らず，漏えい情報の開示を行うランサムウェアグループについて同様の分析が可能であると期待されるが，具体的な調査と適用可能性の検証は今後の課題とする．

7. まとめと今後の課題

ランサムウェアグループ LockBit3.0 のホームページを 166 日間観測し，被害者に関して公開される情報の時間的変化を分析した結果，観測された 1,348 件の被害者のうち，884 件（65.6%）では既に漏えいデータが公開されており，464 件（34.4%）では観測期間中に漏洩データの公開期限へのカウントダウンが観測された．そのうち 71 件（15.3%）ではカウントダウンが停止し，被害者情報の公開が停止されたことから支払いに応じた可能性があることがわかった．また，このうち，公開期限が変更された事例が 38 件（8.2%）確認された．ホームページ上で第三者へ被害者の漏えいデータを販売しているケースは 257 件（19.1%）確認された．公開されたチャット内で示された身代金の金額は 10 万米ドルから 8000 万米ドル（約 1500 万円から約 116 億円）で，平均 453 万米ドル（約 1.5 億円）だった．本報告執筆時点で，は，LockBit3.0 のホームペはテイクダウンされているが，本報告で実施した分析は他のランサムウェアグループの活動把握にも有効であると期待されるため，今後はそれらの観測を行うと共に，他の情報源との突合による観測イベントの意味付けや詳細分析を行う．

謝辞 本研究の一部は JSPS 科研費 21H03444，科研費 21KK0178 の助成を受けて行われた．

文　献

[1] “令和 4 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/R04_cyber_jousei.pdf.
[2] 中須寛人，“【2023 年最新事例】「lockbit 3.0」と各種ランサムウェアによる被害事例,” https://www.daikodenshi.jp/daiko-plus/security/lockbit-3-0/.
[3] T. Reuters, “LockBit digital gang disrupted by international law enforcement in ’Operation Cronos’,” https://www.cbc.ca/news/world/lockbit-hackers-fbi-ransomware-cronos-1.7119651.
[4] “ランサムウェア被害者の知られざるストーリーの解明,” https://blogs.trellix.jp/uncover-the-hidden-story-of-ransomware-victims.
[5] A. Gazet, “Comparative analysis of various ransomware virii,” Journal in computer virology, vol.6, pp.77–90, 2010.
[6] G. O’Gorman and G. McDonald, Ransomware: A growing menace, Symantec Corporation Arizona, AZ, USA, 2012.
[7] M.R.A. Khan, “Understanding impacts of a ransomware on medical and health facilities by utilizing lockbit as a case study,” Security and Privacy, vol.7, no.1, p.e328, 2024.
[8] I.N. Chavez, B. Gelera, K. Casona, N. Morales, I.N. Gonzalez, and N.G. Ragasa, “Lockbit ransomware group augments its latest variant, lockbit 3.0, with BlackMatter capabilities,” https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html.
[9] A. Brandt, “Lockbit 3.0 ’black’ attacks and leaks reveal wormable capabilities and tooling,” https://news.sophos.com/en-us/2022/11/30/lockbit-3-0-black-attacks-and-leaks-reveal-wormable-capabilities-and-tooling/.
[10] “ランサムハッカー集団 lockbit3.0 の脅威分析とその防止策とは,” https://www.txone.com/ja/blog-ja/malware-analysis-lockbit-3-0/.
[11] O. Akinyemi, R. Sulaiman, and N. Abosata, “Analysis of the LockBit 3.0 and its infiltration into advanced’s infrastructure crippling NHS services,” 2023.
[12] T. Meurs, E. Cartwright, A. Cartwright, M. Junger, R. Hoheisel, E. Tews, and A. Abhishta, “Ransomware economics: A two-step approach to model ransom paid,” 18th Symposium on Electronic Crime Research, eCrime 2023, pp.••–••, 2023.
[13] “dperson/torproxy,” https://github.com/dperson/torproxy.
[14] “Selenium ブラウザー自動化プロジェクト,” https://www.selenium.dev/ja/documentation/.
[15] “Beautiful soup,” https://www.crummy.com/software/BeautifulSoup/.
[16] “Blockchain. com,” https://www.blockchain.com/explorer.