マルウェア解析レポート

― Loki Locker の暗号化処理 ―

2023 年 10 月

株式会社ファイブドライブ
〒101-0045 東京都千代田区神田鍛冶町三丁目4番地
TEL: 03-5577-5030/FAX:03-5577-5823

注意事項

本解析はマルウェアやリバースエンジニアリング等に関する高度な知見を有する当社技術者が実施したものであり、本報告書内の記述は、インターネット上にて採取された不審ファイルの解析結果報告という性質上、危険事項等を含むことがあります。本報告書の内容を利用して自身あるいは第三者に損害が発生したとしても、当該損害につき当社は一切その責任を負いません。

目　次

1. ランサムウェア攻撃とLoki Lockerの概要

1.1. ランサムウェア攻撃とその派生

ランサムウェアとは、侵入したコンピュータ内のデータを暗号化し、その所有者に復号を持ちかけて、データの身代金として金銭を支払わせようとするプログラムです。ランサムとは身代金を意味する英単語ransomであり、データを人質に身代金を要求するソフトウェアという意味を持ちます。

ランサムウェアはサーバ内に侵入した攻撃者により直接感染させられるケースや、標的型攻撃メールに添付されて送信されるケース等様々な感染経路が存在します。感染に成功したランサムウェアはコンピュータ上から機密情報を窃取、暗号化します。暗号化により、コンピュータはその機能の多くが実行困難となり、業務等に必要なデータも破壊されるため、業務等に支障をきたします。過去にも、国内外を問わず、ランサムウェアに感染した組織の管理する施設やサービスが正常に機能しなくなり、莫大な経済的損失が生じたケースが多数存在します。そこで攻撃者グループは自らが暗号化したファイルを復号すると持ち掛け、その対価に金銭を支払うよう要求します。近年では、暗号資産での支払いを要求するケースが極めて多くなっています。その他の送金手段と比べ、攻撃者の身元をたどりづらく、被害者にとっても内密に身代金を支払いやすい等の利点があるために選択されているものと思われます。また、機密情報を窃取する場合、身代金を支払わなければ攻撃者グループが管理するリークサイト上にデータを公開すると、二重に脅迫するものも存在します。過去にも政府機関や大企業の機密情報とされるデータが多数リークサイト上に公開されています。そのように二重に脅迫を行うことで、暗号化による被害を受けてもバックアップにより容易に復旧できるような被害者に対しても攻撃として有効に働き、身代金を得やすくするものと考えられます。

ランサムウェアの亜種としては、ワイパーと呼ばれるタイプのマルウェアも存在しています。ワイパーは、ファイルの暗号化を行うものの、対応した復号の仕組みを持たないため、事実上データを削除ないしは完全に破壊しています。ワイパーに暗号化されたが最後、攻撃者であってもデータが復旧できなくなるため、身代金を要求する脅迫の材料としてはランサムウェアの暗号化に劣るものの、破壊活動そのものを目的とする場合にはランサムウェアよりも適しているといえます。このタイプのマルウェアは東京五輪開催期間周辺において、テロ行為のために用いられたことが知られています。テロ行為のように政治的主張や工作を行う上では、復旧を考慮する必要がなく、破壊活動さえ行えば目的を達成できます。ただし、ワイパーの中には、そもそも原理的にデータ復旧が不可能でありながら、身代金を要求するケースも報告されています。多くのランサムウェア攻撃者グループが自分たちの提供する「復号サービス」の信用性向上のために腐心し、ランサムウェアだけでなく被害者へのメッセージも含めて改良を重ねていることを踏まえると、このようなワイパーでランサムウェアのような金銭要求を行うケースは、短期的に金銭を得られればそれでよいという考えで実行されているものと思われます。

さらに、暗号化自体を実行せず、データを窃取するのみに留め、窃取したデータを公開すると脅迫するノーウェアランサムと呼ばれる攻撃手法が日本国内でも報告され始めています。この手法は国外では以前から存在していましたが、これまで日本国内で被害が公表されたケースはそれほど多くありませんでした。今後同手法の被害が日本国内においても増加するおそれがあります。ランサムウェアでは暗号化処理の実行前に相当量の準備が必要であり、実行にも相応の時間や侵入先コンピュータの管理者権限が必要となります。一方で、ノーウェアランサムでは、ランサムウェアと同様にサーバへの侵入やマルウェア感染等、情報を不正に取得する何らかの手段を用意する必要はあるものの、管理者権限なしに重要なデータを取得できる可能性もあり、暗号化処理ほど多大な時間や労力を要することもありません。そのため、単にサーバ等への侵入を金銭の取得につなげるだけであれば、データを窃取して公開すると脅迫する方が確実かつ容易に実行できます。また、ランサムウェアでは、例え被害者の持つデータの暗号化に成功しても、被害者が事前にバックアップを安全な領域に保存していた場合、業務への影響は生じるものの復旧は容易に実行可能なケースが少なくありません。そのため、近年のランサムウェアでは、暗号化に併せてデータの窃取も行い、データを公開すると脅迫するケースが増加しています。ノーウェアランサムの増加は、こういった流れの中で、攻撃者グループにとって暗号化処理は労力に見合った利益を得られないものであり、わざわざ行わなくともデータの窃取のみで脅迫の材料足り得るという認識に変化しつつあることを示唆するものと考えられます。ある意味においては、高度で洗練されたランサムウェアを用いた現代的な攻撃手法から、「秘密を暴露されたくなければ金を払え」と単純に脅迫する、情報化社会の遥か以前から存在する極めて古典的な攻撃手法へ回帰しつつあるともいえます。

また、ノーウェアランサムにおいては、一切サーバ等に侵入せずとも「データを窃取した。身代金を支払わないならデータを公開する。」と単純に虚偽の内容で脅迫を行うことも可能です。十分なIT知識を持たない企業の場合、脅迫に屈してしまう可能性も考えられます。また、調査を行って、本当にデータを窃取された可能性が低いことが判明したとしても、調査コストが生じることは避けられず、業務への影響も生じかねません。また、内部犯によるデータの持ち出しであった場合には、単純にサーバのログ等を確認するだけではデータの漏えいを否定することは難しいケースもあり、正しい対応が困難になるおそれがあります。ノーウェアランサム手法が増加するほど、ランサムウェアの行うものを含めて、脅迫の威力が強まるため、十分な警戒が必要です。

1.2. Loki Lockerの特徴

Loki Lockerはランサムウェアの一種です。似た名称を持つマルウェア及び攻撃グループにLockyやLokiBotと呼ばれるものがありますが、Loki Lockerとの関連性は現在はっきりとは確認されていません。2021年にその存在が確認されたLoki Lockerは、世界的に猛威を振るうEmotetやLockBit等のランサムウェアと比べると、知名度は低くなっています。

Loki Lockerは、そのほかの多くのランサムウェアと同様に、ランサムウェア攻撃を「アフィリエイト」として展開しています。攻撃者グループは、作成したランサムウェアを使って攻撃、ないしは攻撃の手引きをする協力者を募集しており、その働きに応じた報酬を支払うと宣伝しています。このような攻撃形態はRansomware as a Service(サービスとしてのランサムウェア)、略してRaaSと呼ぶこともあります。

このようなRaaSは、アフィリエイト参加者に対する求心力を保つことや感染したユーザに脅威と認識させて身代金を支払わせるために、積極的に攻撃グループの売名に努めています。ランサムウェア以前のマルウェアには感染したこと自体を隠蔽しようとするものが少なくない中、多くのランサムウェアは自らその名前とともに感染したことをユーザに通知します。感染の通知そのものは身代金の支払いにつなげるために必要ではありますが、攻撃者グループの名前を前面に押し出してアピールする挙動は、当該攻撃者グループのランサムウェアに感染した被害者が増加していることを広く知らしめることで、利益のために攻撃に協力するものを増やすとともに、被害者に対しての脅迫の威力を強める狙いがあると考えられます。

ただし、RaaSとして活動を展開するランサムウェアの中では、Loki Lockerは活動規模が大きくならないように制限していると見られています。過去のセキュリティ研究者の分析によると、アフィリエイト協力者は2021年段階で30人前後と見られています。仮に現在その規模を拡大していたとしても、報告されている感染事案件数やインターネット上で発見される検体の数等を見るに、大きく変化していないものと考えられています。参加者を選定している基準等は不明ですが、参加者の質を確保することで、いたずらに大規模な被害を引き起こして世間や警察機関等からの注目を集めてしまうことがないようにする目的があるのではないかと考えられます。あるいは、現在RaaSとしての稼働は試験段階にあり、本格的な攻撃活動を行っていないという可能性も考えられます。

ほかのランサムウェアにおいても、アフィリエイト協力者による攻撃対象の選定に細かく制限を設けて注目を集めないように努めているものは少なくありません。攻撃対象は基本的にアフィリエイト参加者が選択してもよいとしつつ、攻撃が人命に直接関わる医療施設への攻撃を禁じる等のルールを設けている攻撃者グループも存在します。このようなルールは攻撃者グループの良心や倫理によるものではなく、世間から注目を集めすぎないようにするためのものであると考えられます。攻撃者グループ名やランサムウェア名を大きくアピールするからこそ、そのランサムウェアによって人命に関わる事件が立て続けに起きれば、アフィリエイト協力者を集めづらくなり、警察やそのほか法的機関も対処の優先度を大きく引き上げることが予測されるからです。実際、過去にEmotetと呼ばれるランサムウェアが世界的に

大きな被害をもたらしたため、欧州警察機構主導の制圧作戦によって一度制御サーバ拠点を制圧されたことがあります。Loki Lockerは、現在までのところ、そのような事態を招かないように、過度な注目を避ける傾向が強いRaaSであると考えられます。その理由は、小規模で長期間活動すること、試験段階にあること、あるいはほかに何らかの理由がある可能性もありますが、それらの理由にかかわらず現在に至るまでLoki Lockerは攻撃者グループとしては知名度がそれほど高くありません。

一方で、Loki Lockerでは、近年のランサムウェアに多く見られる、データを窃取して公開すると脅迫する動きが見られません。今回弊社にて解析を行った検体においても外部へ暗号化対象のファイルの内容を送信するような挙動は見られず、データの公開を行うリークサイトも、2023年10月現在、確認されていません。

2. Loki Lockerの感染経路と対策

2.1. 感染経路と感染活動

Loki Lockerの侵入手段として特徴的なものは現在のところ知られていません。ほかのマルウェアと同様に、様々な手段でコンピュータへ侵入を試みるものと思われます。

一般的なマルウェアは、インターネット上の不審ファイルや電子メールの添付ファイルに潜むマルウェア本体、あるいはマルウェアの侵入を手引きするプログラムによる感染を行うことがよく知られています。それに限らず、ソーシャルエンジニアリングと呼ばれる信頼されている個人や組織になりすましてアクセス権を不正に取得する手法や、公開されているWebサーバの脆弱性を突いて設置したバックドア(攻撃者の侵入を容易にするプログラム。裏口を意味する英単語Backdoorに由来する。)を用いた手動での侵入等、多岐に渡ります。

しかし、先述のとおり、Loki Lockerは活動を小規模なものに留めているため、大規模にランサムウェアをばらまくような感染手法を取るとは考えにくく、攻撃対象を十分に選定し、侵入と攻撃を試みるものと思われます。また、ばらまき型攻撃において、被害者にマルウェアをダウンロードさせるURLは世界中の有志によって報告され、データベースサイトに記録されていますが、そのようなデータベースサイトでLoki Lockerはほとんど確認できません。

Loki Lockerには、侵入したネットワーク内で感染を広げる機能や、脆弱性等を利用して特権を強制的に取得する機能は確認されていません。アフィリエイト協力者がほかの攻撃ツールやサーバの設定不備、脆弱性等を利用して不正に侵入した後、不正侵入を金銭の取得へつなげるためにLoki Lockerを利用するのではないかと考えられます。

攻撃者により侵入を受けた後、Loki Lockerは内蔵されたディスク及びネットワークスキャンを行うツールを実行し、侵入した環境についての情報を集めます。この情報を基に、攻撃者はLoki Lockerをどのように実行するか判断すると考えられます。

全ての準備が整うと、Loki Lockerは暗号化攻撃を開始します。暗号化したコンピュータにはデスクトップ背景にそれを示唆するメッセージを表示させ、身代金の支払い方等を示す小規模なプログラムを配置します。一通り暗号化が完了した後も、コンピュータの監視は継続され、新たなファイルを検出するたびに速やかに暗号化処理が実行されます。

2.2. 対策手段

一度ランサムウェアの侵入を許すと個々のコンピュータにセキュリティ対策を導入していたとしても、感染は瞬く間に組織全体へ広がってしまう可能性があり、対策は困難です。ランサムウェアの被害を防ぐための対策だけでなく、被害に遭った際も影響範囲を最小限に抑えるという観点に立った対策が必要です。

まず、ランサムウェア対策に限らず、不審なファイルを開かないよう、セキュリティ教育を組織内で徹底することが非常に重要です。しかしながら、近年では不正に取得したメール履歴などを基に非常に巧妙ななりすましメールを作成し、マルウェアを添付するケースが確認されています。そのため、特定の組織を狙った巧妙な攻撃においては、メールの文面やタイトルだけで不審な添付ファイルであると判断することが難しくなりつつあります。また、実在の個人や組織を名乗り、複数回のやり取りを経て信用を得てからマルウェアを送信するケースも存在します。そのため、旧来の不審であることが明確な迷惑メールのようなケースのみを想定している場合、思わぬ被害が生じるおそれがあります。

また、システムへのアクセスに必要なパスワードに脆弱なものを設定できないようにすることも重要です。最低限必要なパスワード長や文字種数を多くすることが重要です。加えて、ありふれた英単語や日付、名前、商品名のような単語は攻撃者のパスワード辞書に登録されていることが多く、辞書攻撃に対して脆弱になるため、そのような文字列をパスワードに利用しないようセキュリティ研修等を通し組織内に徹底していく必要があります。さらに、複数サービスでのパスワードの使いまわしは、いずれかのサービスで漏えいした場合に、パスワードを使いまわしている全てのサービスで不正アクセスの可能性が生じます。これを防ぐための定期的なパスワード変更も、変更頻度が高い場合にはユーザが最新のパスワードを覚えることが難しくなり、覚えやすい脆弱なパスワードを設定する可能性が高くなることにも注意が必要です。

さらに、システム内の各アカウントを見直すことも重要です。アクセス権限が不必要に与えられていないか、退職者のアカウント等の既に使われていないものが残っていないか確認しなければなりません。これらはランサムウェアに限らず内部不正や不注意による情報漏えいの対策にもなります。

サーバをはじめとするコンピュータに対し、常に最新のセキュリティ対策を実施し続けることも重要となります。攻撃者とセキュリティ技術者の攻防は日進月歩であり、それまで安全とされてきたソフトウェアや設定が、次の日には危険であるとされることも少なくありません。定期的な点検や脆弱性診断を行うことが重要です。

そして、上記のような対策を万全に施したとしても、万が一侵入される可能性は否定できません。攻撃者グループが多額の暗号通貨を餌に攻撃を手引きする協力者の募集を行っていることや、脆弱性が公式に報告、修正されるよりも前にその脆弱性を利用した攻撃が開始されるケースが存在することが理由です。そのような場合にも致命的な損害を被ることがないよう、重要なデータは定期的にバックアップを作成し、ネットワークに接続されないオフラインの環境に保存しておくことが必要です。ネットワークに接続されたバックアップは、ネットワーク内に感染を拡大するランサムウェアにより無効化される可能性が高くなります。また、バックアップも感染しているという最悪の事態を避けるために、最新のものだけでなく過去の複数の時点でのバックアップを用意することが重要です。

2.3. 留意事項

本報告書は解析実施時点におけるマルウェア・脆弱性情報や攻撃手法に関する情報を基に得られた結果を述べたものであることをご理解ください。新しい脆弱性や攻撃手法は日々発見されており、解析実施時点では被害が生じないと判断された対象においても、将来において新たな脆弱性や攻撃手法が報告され、それによりマルウェアによる被害が生じる可能性があります。

本報告書は弊社解析担当者がインターネット等で採取した複数の検体に対して解析を実施した結果を記載したものであり、解析を実施した環境において実際に確認された挙動を記載しています。本解析においては、マルウェアが利用するソフトウェア等の脆弱性が存在する場合、対策を講じないために生じ得る被害も含めて報告しています。

本報告書には、マルウェア内部の有害なコードに関する説明が存在します。暗号化処理に関するコードについては、直接攻撃に利用できるような箇所が多いため、広く公開する文書であることを踏まえて、新たな攻撃に悪用されることがないようにコードそのものの記載を控えております。あらかじめご了承ください。また、入手経路を問わず、正当な理由なく、悪意あるコードを実行または実行する目的で第三者へ提供することはお控えください。実行された環境に被害が生じるのみならず、不正指令電磁的記録に関する罪に問われるおそれがあります。また、同様に報告書内にマルウェアに関連するものとして記載された URL が存在する場合、当該 URL へのアクセスもお控えください。マルウェアがダウンロードされる等の被害が生じるおそれがあります。なお、不審ファイル内部で検出された URL を掲載する際は、その URL の有害度によらず、誤ったアクセスを防ぐため、URL 文字列中の「.」(ドット)の文字を角括弧で挟んで記載しています。

本報告書において記述されている不審ファイル危険度の評価や検出されたマルウェアによるリスク内容は、運用の方針（セキュリティポリシーなど）・環境・状況等により変化します。ただし、本報告書では、セキュリティ解析の性質上、運用の方針（セキュリティポリシーなど）・環境・状況等は考慮せずに解析対象ファイル単体の視点から不審ファイル危険度の評価やリスク内容を記載していることをご理解ください。そのため、マルウェアへの対応につきましては、運用の方針（セキュリティポリシーなど）・環境・状況等を考慮していただき対応策を検討してください。

3. Loki Lockerの解析

3.1. 検体ファイルについて

2023 年 10 月現在まで、Loki Locker はばらまき型の攻撃ではほとんど確認されておらず、個別に攻撃者がサーバ等に侵入を行い感染させるケース等が主な感染経路と考えられています。そのため、暗号通貨のマイニングを不正に行う CoinMiner 等と比較すると、インターネット上で採取できる検体も非常に少数となっています。今回の解析では、数か月前から 1，2 年前までの検体を複数確認していますが、感染したコンピュータに関する情報の収集方法等で多少の挙動の変化が見られるものの、全体の動作としては著しい変化は確認されませんでした。解析対象の中には、有志によってアップロードされたファイルも含むため、実際に攻撃者が侵入したサーバで感染させる場合の手順等について、確実に言い切れることはそれほど多くありません。しかし、今回の調査では、Loki Locker 本体だけでなく、Loki Locker 本体をリソース領域に暗号化した状態で格納し、実行時にメモリ上に展開して起動するタイプのファイルも確認しています。そのようなファイルの場合、暗号化を解除するか、メモリ上に展開された後にメモリダンプを行うことで、マルウェアの核心部分を保存することが可能です。

なお、本章で説明する検体の挙動については、できる限り検出された日付が新しいものによく見られるものを中心に記載しています。

3.2. 検体ファイルの特徴

Loki LockerはMicrosoft社の提供する.NETを利用して作成されています。作成にはC#言語が用いられているものと見られ、その内部では.NETの機能を利用して、脅迫に用いるC#で記述された小さなプログラムを新たにコンパイルして作成することも確認しています。

.NETを利用したプログラムでは、基本的にソースコードに記載した変数や関数、クラス等の名前がそのままコンパイル結果のバイナリファイルにも含まれてしまいます。これらの名前を分かりやすいものにすることは、プログラムの開発においてバグを生じにくくし、安定した保守を行うために重要です。しかし、変数名や関数名がバイナリ内部に残ると、リバースエンジニアリングを行う解析者にとってもコードの内容を把握しやすくなり、解析を容易にします。そこで、攻撃者グループは難読化ツール等を利用して、変数名や関数名をランダムな文字列に置き換えるなどして対策しているケースが多く見られます。この対策は、マルウェアに限らず一般企業が有償で提供するプログラムにおいても、リバースエンジニアリングへの対策として実施されています。Loki Lockerについても、今回採取した検体は全て難読化処理が実施されていました。ただし、2022年時点ではC#の難読化ツールConfuserExで動作するよう設計された仮想マシンKoiVMを利用していたようですが、今回採取した検体の中には、そのような痕跡が見られないものも存在しています。過去のLoki Lockerの難読化の解除方法が既によく知られたものとなったため、新たな難読化方法を講じてきた可能性が考え

られます。ただし、今回の検体については、オープンソースやフリーツールとして提供されているプログラムを用いることで容易に難読化解除可能であるため、必ずしも難読化の解除を困難にする目的で変更されたとも言い切れません。

関数名や変数名、クラス名の難読化だけでなく、関数およびメソッドの呼び出しについてもC#のDelegateを利用しつつ、各Delegateクラスがどの関数またはメソッドを呼び出すのかを動的な値を基に決定するように記述することで、静的解析で処理を追跡するために大きな労力がかかるようにされています。同様に、Loki Locker内で用いる数値や文字列などの多くの定数値もまた動的に生成もしくはリソース領域から復元されるようになっており、解析に時間がかかるよう工夫されています。

3.3. 暗号化の準備処理

検体が実行されると、まず多重起動を防ぐ処理やエラーハンドラの準備等を行います。その後、Loki Lockerの設定を記載したファイルを検索し、発見できた場合はそれらの設定を利用します。今回の検体ではloki.txtやconfig.Lokiという名前のファイルの存在を確認することによって判断します。これらファイルが存在しない場合は、Loki Locker内部に記載された設定を利用するものと思われます。

次いで、自身のコピーをwinlogon.exeという名前でコンピュータのスタートアップに関するフォルダに作成していきます。このファイル名は、Windows正規のプログラムの名前であり、自身を隠蔽するために用いていると思われます。なお、このファイル名については検体ごとに異なる可能性があります。コンピュータの設定にもよりますが、スタートアップに関するフォルダは、配置されたプログラムをコンピュータの起動時に自動的に実行するために利用されます。各検体でコピーファイルの配置先として主に指定されていたフォルダは以下のとおりです。

フォルダ指定値	解析環境におけるフォルダパスの例
SpecialFolder.Startup	C:¥Users¥[UserName]¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup
SpecialFolder.CommonStartup	C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥Startup
SpecialFolder.ApplicationData	C:¥Users¥[UserName]¥AppData¥Roaming
SpecialFolder.CommonApplicationData	C:¥ProgramData
SpecialFolder.SystemRoot	C:¥Windows

こうして作成したコピーを利用するために、Windowsのタスクスケジュール機能やレジストリ中の実行時の処理に関する項目を利用し、コンピュータがシャットダウンされた場合でも、次の起動時に自身が再実行される持続性を確保しています。このレジストリのキーの中に「Michael Gillespie」というものがあります。これは、著名なセキュリティ研究者の名前であり、Loki Lockerがレジストリのキーとして利用する特有な文字列としても知られています。このようなセキュリティ研究者に対する挑発ともとれるような記述は、過去ほかのマルウェアでも報告されているものの極めて少数です。

上記のように自己の持続性を確保した後に、Loki Lockerは暗号化処理を成功させるための環境整備および環境情報の収集に移ります。

まず、自身のリソース部分に画像形式で保存されていたLoki Lockerのアイコンを取り出して、ランダムなファイル名を与えて保存します。同様にリソース部分からプログラミング言語C#で記述された文字列を取り出し、.NET環境を利用することでコンパイル処理を実施し、生成された実行ファイルにランダムなファイル名を付けて保存します。

```
using System;
using System.Diagnostics;
using System.IO;
using System.Runtime.InteropServices;

namespace Loki
{
    class Natives
    {
        [DllImport(\"user32.dll\", SetLastError = true, CharSet = CharSet.Auto)]
        public static extern int MessageBox(IntPtr hWnd, String text, String caption, uint type);
    }
    class Program
    {

        static void Main(string[] args)
        {
            Natives.MessageBox(IntPtr.Zero, \"This file and all other files in your computer are encrypted by Loki locker.\\r\\nIf you want to
            string filename = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData),\"info.Loki\");
            if (File.Exists(filename))
            { Process.Start(\"mshta.exe\",\"\\\"\" + filename + \"\\\"\"); }
        }
    }
}
```

図 1 コンパイルされる C#のソースコード

また、この際に被害者への脅迫に用いるHTMLアプリケーションファイルも作成します。なお、被害者固有のIDのように見える数値は、Windowsの保存されたドライブにWindowsが独自に割り振ったIDを用いていました。工場での製造時に割り振られる固有のシリアルナンバー等とは異なり、被害者間で重複する可能性は極めて低いものの、ゼロではありません。また、コンピュータを調査して初めてこの値が判明するため、検体によってはこの値を攻撃者のC2サーバ等へ送信する機能を確認しています。送信に失敗した場合や送信機能を利用しない場合は、攻撃者が侵入時にあらかじめこの値を調査して記録しておくことで被害者を識別しているか、攻撃者へ被害者が連絡することで初めて被害者を識別するIDとして働くものだと思われます。

以上の処理を終えたところで、対象ファイルは自身に与えられた権限を確認します。管理者権限でない場合は、別のプロセスを作成し、そのプロセス内で管理者権限を用いて自分自身を実行しようとします。一部のファイルに対する暗号化処理やその準備に必要なセキュリティ機能の無効化等には、基本的に管理者権限が必要となることが理由であると考えられます。仮に管理者権限を得られなかった場合、数秒の待機を経て、繰り返し別のプロセスを作成し、そのプロセス内で管理者権限を用いて自分自身を実行しようとします。

無事に別プロセスで管理者権限を得られたと判断した場合、管理者権限を得られていない元の検体はプロセスを終了するための準備を行った後に、その動作を停止します。今回採取した検体においては、何らかの脆弱性を利用して管理者権限を奪取するような処理は見られませんでした。そのため、攻撃者が実際にコンピュータに侵入し、管理者権限を取得できるようになった状態で、手動で対象ファイルを実行する、あるいはユーザに誤って起動させ、管理者権限の付与を許可させることで感染させると考えられます。ただし、今後新たな脆弱性が感染手段として利用される可能性を否定するものではありません。

管理者権限で実行されている場合は、自身を別プロセスで再実行することなく、そのまま処理を続行します。権限確認後、検体ごとに多少処理の有無や実行方法等が異なることはあるものの、おおむね以下のような処理を実行していました。なお、処理自体は検体内部に記載されているものの、必ずしも暗号化処理に必須ではないものについては設定に応じて処理を実行しないケースも存在するため、実際に攻撃に使用される際に実行される処理と解析環境で実行された処理は異なる可能性があります。

- 偽の Windows Update 画面を表示し、挙動の不審な点を隠蔽
- 暗号化処理を妨げる可能性があるプロセスやサービスを調べ、強制終了
- Windows のタスクマネージャーを強制終了
- スタートアップフォルダにタスクマネージャー無効化 bat ファイルを配置
- システムの回復ポイントやゴミ箱フォルダの中身の削除
- Windows Defender のリアルタイム保護機能および検出サンプル自動送信の無効化
- Active Directory に関する設定を変更
- ボリュームおよびネットワークのスキャン並びに検出されたボリュームのマウント
- ディスクの使用中の容量、メモリ容量、CPU 情報、タイムゾーン等を取得
- 感染したコンピュータへアクセスする際に必要なグローバル IP アドレスを取得
- 環境情報を暗号鍵の作成に用いるために新規のレジストリに保存

これらの処理を終えると、Loki Locker は暗号化処理を開始します。

3.4. 暗号化処理全体の流れ

暗号鍵を生成するために必要な情報を用意したところで、対象ファイルは実際にファイルの暗号化処理に移ります。暗号化処理はスキャナ機能によって強制的にマウント及び表示させた各ドライブに対して順次実行されます。実行対象のドライブは、開始時に状態を調査され、空の CD-ROM 等の暗号化対象として不適切なものは取り除かれます。

暗号化処理は始点となるフォルダが複数指定されており、そのフォルダから更に内部のフォルダへと暗号化処理を展開していきます。ただし、一部フォルダでは直下のファイルのみを暗号化し、サブフォルダに関しては一切暗号化を行わないケースも見られました。

確認された検体の 1 つを例にとると、まず Windows が SpecialFolder.SystemX86 という値で認識するフォルダを含むドライブから暗号化を開始します。これは、一般的な 64bit の Windows コンピュータでは 64bit 用システムフォルダとなるため、Windows が保存されたドライブを特定するためにこのようなドライブ選択を行うものと思われます。これは一般的に C ドライブであることが多く、確認した検体は内部のサブフォルダまで暗号化処理は実施せず、C ドライブ直下のファイルのみを暗号化しています。個々のファイルの暗号化処理については次節で記述します。

その後、検体はユーザプロフィールに関するフォルダ配下のサブフォルダを順に走査し、サブフォルダの内部に含まれるフォルダの中まで含めて、全て暗号化していきます。この際、AppData という名前のフォルダは暗号化処理の対象としないよう設定されていました。このフォルダには様々なアプリケーションが利用するデータが保存されていますが、Loki Locker が持続性確保のために自らのコピーを保存する場所でもあります。

次に、実行中のドライブのフォルダ構造のうち、一番上部に当たるフォルダから暗号化を開始します。このドライブ直下は最初に暗号化処理を実施していますが、このタイミングではサブフォルダの内部まで含めて暗号化処理を実施します。ただし、Windows フォルダ、EFI フォルダ、ゴミ箱フォルダおよびさきに処理済みの Users フォルダは暗号化対象から除外しています。ゴミ箱フォルダは事前の準備処理により内部が既に削除済みであり、処理が不要なため除外されるものと思われます。既に暗号化処理を実施済みの Users フォルダは不要な処理を省いて処理時間を短縮するために除外しているものと思われます。そのほかのフォルダは、コンピュータの動作に関与する重要なファイルが含まれており、暗号化することでコンピュータが破壊されることがないよう除外しているものと思われます

多くのランサムウェア攻撃者にとって、攻撃は破壊や政治的主張のための手段ではなく、身代金を得るためのものです。身代金を要求するためには、コンピュータを完全に破壊してしまうと都合が悪く、最低限 Windows が機能する程度にはコンピュータが処理を継続できる状態が理想的であるからです。

暗号化処理は、最後に Windows が ProgramFiles という値で認識しているフォルダに対して実行されます。これは、近年の一般的な Windows の環境では C:¥Program Files(x86)フォルダが指定されていることが多く、ユーザが独自にインストールしたプログラムなどが保存されています。先述のとおり、実行可能ファイルの多くは暗号化を免れますが、実行可能ファイルが正しく動作するために参照する設定ファイル等は暗号化の対象となるため、このフォルダを暗号化することで Windows の中心機能ではないプログラムの多くが正常に実行できなくなります。

上記の流れは、Loki Locker が起動している限り、永続的に続けられます。そのため、感染後に新たにファイルを作成等した場合、Loki Locker はそのファイルを検出し直ちに暗号化処理を実行します。また、脅迫文は、復号を望むならファイル名を変更してはならないと注意していますが、後述するように暗号化処理の実施可否を拡張子やファイル名から判断しているため、複数回暗号化処理が実行されて復元できなくなることや、Loki Locker の設定情報などが暗号化されてしまうことを防ぐ目的があると思われます。なお、これらは攻撃者の良心に基づくものではなく、あくまで身代金を支払わせるために重要な「復号サービス」の信用性が不要に低下しないようにするためのものです。

初回の暗号化処理完了後、対象ファイルはデスクトップ背景画面を独自のものに変更します。このデスクトップ背景には連絡先メールアドレスや、被害者 ID が示されていますが、アフィリエイト参加者や被害者により異なるこれらの情報を含めるために、背景画像は Loki Locker 起動後に動的に作成されています。なお、連絡先メールアドレスのドメインは様々なケースを確認しており、本報告書で示したものに限りません。

図 2 暗号化されたことを通知する背景画像

その後、HTML アプリケーションを実行することで、ユーザに Loki Locker への感染と暗号化を通知し、身代金の支払いを要求します。また、同時に Windows へのログイン時のメッセージや暗号化処理を完了したドライブのラベルを感染の通知メッセージに変更し、ユーザが確実に感染に気付くようにします。

図 3 暗号化処理された後に PC を起動しログインすると表示されるメッセージ

最後に、暗号化処理を実施したドライブに対してデフラグ処理を実施します。デフラグ処理は、ドライブ内の保存領域の断片化を緩和するデータ整理処理です。

Loki Locker は自身を持続化させる処理を実行しているため、例えコンピュータをシャットダウンしたとしても、暗号化処理は再度コンピュータが起動した際に再度実行されます。

3.5. ファイル暗号化処理

個別のファイルの暗号化処理については、検体の一つを例にとると、暗号化処理は以下のような手順で実行されます。検体によっては処理の細部や順序が異なる可能性があることにご注意ください。

まず、対象ファイルパスから拡張子を取得し、.Loki であれば暗号化処理を行わずに終了します。拡張子.Loki は Loki Locker が暗号化処理を実施したファイルや自身に関する情報を保存したファイルに用いられます。そのため、攻撃者としても暗号化を望まないファイルの識別に用いていると思われます。

次に、対象ファイル名が Restore-My-Files.txt、または info.hta かどうか確認し、もしそうであれば暗号化処理を行わずに終了します。これらのファイルは、攻撃者がユーザに対して復号のための手続きを記載したものであり、暗号化を行うべき対象ではないため、除外しているものと思われます。

その後、対象ファイルの存在するフォルダ内に Restore-My-Files.txt という名前のファイルが存在しない場合、新たに復号のための手続きや連絡先を記載したファイルを作成し、Restore-My-Files.txt という名前で保存します。

さらに、対象ファイルの拡張子が.exe、.dll、.msi、.com であるか確認し、もしそうであれば暗号化処理を行わずに終了します。これらは Windows における実行可能ファイルおよびライブラリファイル等を示す拡張子です。脅迫して身代金を支払わせるために必要な Web ブラウザ、メールクライアント等の拡張子としても一般的であるとともに、Loki Locker 自身の拡張子としても用いられるため、暗号化後にユーザが身代金を支払うことが困難にならないようにする目的があると思われます。また、Windows の重要な機能を担うプログラムについてもこれらの拡張子を用いていることが多く、誤ってコンピュータに致命的な損害を与えないようにするためでもあると考えられます。

対象ファイルが以上の除外判定を通過した場合、対象ファイルを開き、そのファイルサイズを取得します。今回解析した検体においては、1572846 バイトを閾値としており、ファイルサイズがこの値より大きいか否かで処理が変わります。

ファイルサイズが 1572846 バイト以下である場合、検体は AES 暗号の共通鍵の生成に必要な乱数や、ノンス、認証タグとして用いる乱数を BCryptGenRandom により作成します。それらの乱数を基にして、AES 暗号に用いる共通鍵を、ChainingMode に Galois Counter Mode(GCM)を設定して作成し、対象ファイル全体を暗号化した内容で上書きします。暗号化終了後、共通鍵は直ちに廃棄されます。

ファイルサイズが 1572846 バイトよりも大きい場合、Loki Locker はファイル全体に暗号化を実施せず、ファイルの先頭、末尾、中間からそれぞれ 262144 バイトを暗号化します。それぞれの部分の暗号化方法は、先述したファイル全体を暗号化する際の処理と同様です。

このようなファイルサイズに応じた処理の変更は、暗号化処理にかかる時間を短縮するためのものです。ファイルの暗号化処理は少なくない時間を要し、また感染したコンピュータの性能は高いものとは限らないため、このような工夫を講じているものと思われます。なお、ファイルの一部のみの暗号化であっても、暗号化する領域の大きさと場所を選定することで、ほとんどの場合ファイルは本来の用途には利用できなくなるため、身代金を要求するためにコンピュータを正常に利用できない状態にするという攻撃者の目的を達成することができます。

上記の処理の分岐のいずれの場合においても、暗号化処理が完了すると Loki Locker は共通鍵の生成やノンス、認証タグとして用いられた乱数をまとめて RSA 暗号化処理を実施し、暗号化したファイルの末尾に付与します。暗号化したこれらの乱数はファイルを復号する際に再び共通鍵の生成やノンス、認証タグとして用いるものと考えられます。実際に攻撃者が復号を行うかは定かではありませんが、少なくとも構造上復号が可能でない場合、攻撃者が身代金と引き換えに提供すると謳う「復号サービス」の信頼度が著しく低下するため、そのような事態を避けるためにも必要な処理です。

ここで利用される RSA 暗号は、AES 暗号と異なり、暗号化と復号に用いる鍵が異なり、暗号化に用いる鍵では復号できません。今回のようなケースでは、暗号化に用いる鍵を公開鍵とし、復号に用いる鍵が秘密鍵として扱われます。公開鍵を基に秘密鍵を現実的な時間で推測することは、現在実用化されている計算機技術では難しいため、公開鍵はその名のとおりに公開してもよいとされています。この仕組みは、インターネット上でサーバ等と通信する際にも用いられています。自身へ送信するデータを暗号化してもらうために暗号鍵を公開し、その復号に用いる鍵は秘密にしておくことで、誰でも自分に情報を安全に送信できるようにしながらも、その内容は正規の受信者である自分のみが閲覧可能にすることができます。また、この方式には事前に鍵を共有する必要もないという利点もあります。この仕組みを悪用したのがランサムウェアです。

今回利用されている暗号鍵は、Loki Locker 内部に保存されている 5 つの公開鍵と、事前準備段階で収集した感染したコンピュータの環境情報を基にして新たに作成されていました。推測ではありますが、恐らくこの 5 つの公開鍵は、検体によらずアフィリエイト参加者ごとに同じ値であり、したがって対応する秘密鍵も検体によらず同じ値ではないかと思われます。このように同じ公開鍵を用いて対象ファイルごとに異なる暗号鍵を作成することにより、ある暗号化されたファイルの復号鍵を万が一入手できたとしても、ほかのファイルでは異なる鍵が用いられているために復号できないという困難な状況を作り出すと同時に、攻撃者の持つ秘密鍵はマスターキーのように働き、全てのファイルを自由に復号できる仕組みであると思われます。

最後に暗号化処理および鍵情報の付与が完了すると、Loki Locker は対象ファイルの名前に連絡先メールアドレスや被害者 ID を付与し、拡張子を.Loki に変更し、被害者が被害を認識しやすくするとともに、多重に暗号化してしまうことを防止しています。

4. 付録

4.1. マルウェアの基礎知識

サイバー攻撃にも様々なものがありますが、IPA（独立行政法人情報処理推進機構）が毎年発表している「情報セキュリティ 10 大脅威(2023)」の中でも、組織向け脅威の上位 3 位が、侵入経路は様々なものの、マルウェアによる脅威となっています。

マルウェアとは、英語で「悪意のある(malicious)」と「ソフトウェア(software)」が組み合わさって作られた言葉で、「ウイルス」「ワーム」など、悪意のあるソフトウェア全般を指します。

日本国内では、刑法第 168 条の 2「不正指令電磁的記録作成等」等で、マルウェアに当たるプログラムを「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」と定め、その作成や実行、実行目的と知りながらの提供、取得、保管を禁じ、罰則を定めています。また、マルウェアの動作によって、詐欺や名誉棄損、わいせつ物頒布等の罪に該当する可能性もあります。

ただし、この定義は単純ではなく、専門家でなければ判断が困難なものもあります。例えば、ハードディスク内の全てのファイルを消去するプログラムを考えます。その内容について説明した上で提供した場合は、使用者は意図して使用したことになります。一方で虚偽の説明を行い、相手が実際の動作を知らない状態で誤って実行するよう仕向けた場合は、全く同じプログラムでも「不正な指令を与える電磁的記録」と判断される可能性があります。

また、コンピュータプログラムにおいてはバグによる不具合は、程度によらず不可避なものと許容されています。そのため、不具合によって意図せぬ現象が生じた場合は「不正な指令を与える電磁的記録」と判断される可能性は低いといえます。しかし、不具合によって意図せぬ現象が生じ、その結果として多大な損害を与える可能性が極めて高いことを承知の上で、その旨を伝えずに他人に当該プログラムを提供した場合には、事実上の「不正な指令を与える電磁的記録」を、他人を害する目的で提供したと判断される可能性を否定できません。

マルウェアはその活動方法や目的によって分類されています。活動方法による分類は「ウイルス」「ワーム」「トロイの木馬」です。

「ウイルス」は生物に感染するウイルス同様、単独では活動できず、ほかのファイル等に寄生して活動・拡散します。ただし、生物に感染するウイルスとは異なり、自己複製機能を持っていません。

「ワーム」は単独で活動可能であり、自己を複製して感染を広げていきます。USB フラッシュメモリ等を通して感染するマルウェアはこのタイプであることが多くなっています。

「トロイの木馬」はギリシア神話のトロイア戦争の物語が由来となっています。攻撃対象端末に秘かに忍び込み、無害なプログラムやデータファイルを装って潜伏します。その後、何らかのきっかけで活動を開始し被害をもたらします。現代では最も多数のマルウェアが該当します。

目的による分類は多岐に渡り、一つのマルウェアが複数のカテゴリに属することもあります。ランサムウェア、スパイウェア、キーロガー、ダウンローダー、ボット等が挙げられます。以下にその一部を示します。

分類	被害内容
ランサムウェア	ファイルを暗号化し、コンピュータの起動や動作を困難にした後、復旧を謳い身代金を要求します。さらに情報を公開すると脅迫するものも増加しつつあります。近年では暗号化を実行せず、データを窃取して脅迫する手法も増加しつつあります。
スパイウェア	潜伏してコンピュータの利用情報等を攻撃者に送信します。機密情報が漏えいし、さらなる攻撃の手掛かりを与えることにもつながります。
キーロガー	スパイウェアの一種で、特にキーボードの打鍵回数、打鍵履歴等を窃取します。パスワードや暗証番号の窃取が多くみられます。銀行口座や決済サービスを利用した不正送金や、Web サービスやオンラインゲーム等のアカウントの乗っ取りのために利用されるケースが見られます。
バックドア	攻撃者が侵入、あるいはほかのマルウェアを感染させるための勝手口として機能します。バックドアを設置され、それが有効に機能している状態では、バックドアを設置した攻撃者からのあらゆる攻撃を受ける可能性が高まり、甚大な被害が生じる可能性があります。脆弱なサーバに仕掛けられるケースがよく見られます。
ダウンローダー	単独では破壊活動や情報窃取は行わず、攻撃者のサーバからほかのマルウェアをダウンロードする手引き役です。
ボット	感染した端末は、攻撃者の指示により、第三者のシステムなどを攻撃する際の踏み台や、DDoS 攻撃のためのデータ送信端末として利用されます。日本国内でも、過去に踏み台として利用された端末の所有者が誤認逮捕された事件が存在します。
アドウェア	不正な広告や料金を請求する表示を画面上に表示し続けます。不正な表示を消すためにはコンピュータに関する知識が多少必要ですが、料金請求に応じたり、表示された連絡先へコンタクトを取ったりしなければ、比較的実害は生じにくいといえます。
ドロッパー	ダウンローダーに似ていますが、外部からマルウェアをダウンロードせず、自身にほかのマルウェアを内包しています。侵入後に内包するマルウェアを引き出し実行します。

近年のマルウェアの目的は、機密情報の窃取や情報・システムの停止や破壊、詐欺や脅迫による金銭取得等が代表的です。以前は攻撃者が自己の技術をひけらかす愉快犯が多いとされていましたが、近年では金銭等の利益を目的としたマルウェアが増加しているといわれています。

マルウェアについても、Web サイトやソフトウェアの脆弱性と同様に、攻撃側と防御側のいたちごっこが続いていますが､近年では特にウイルス対策ソフトの検知を逃れるために様々な細工を施したマルウェアが増加しています。

以上