初期アクセス	実行	永続化	権限昇格
T1189 - ドライブバイ攻撃（Drive-by Compromise） Agendaランサムウェアは、ドライブバイダウンロード、偽装されたクローンサイト、ホストされたファイル、スクリプトによるウェブ配信、または侵害されたシステムを通じて配布されることが確認されています。 T1091 - リムーバブルメディアによる拡散（Replication Through Removable Media） USBドライブやCDなどのリムーバブルメディアを介して、自動実行されるペイロードを生成する機能を備えています。 T1078 - 有効なアカウントの悪用（Valid Accounts） 窃取された認証情報やプロセストークンのなりすましを通じて取得した、侵害済みのアカウントを利用します。 T1566.002 - フィッシング：スピアフィッシングリンク（Phishing: Spearphishing Link） 悪意のある添付ファイルやリンクを含むメール、または偽のCAPTCHAを用いたソーシャルエンジニアリングによって侵入する場合もあります。	T1059 - コマンドおよびスクリプトインタープリタ（Command and Scripting Interpreter） Agendaランサムウェアの各種バリアント（Go、Rust、Linux）は、設定や実行のために複数のコマンドラインパラメータを受け付けます。これには、暗号化の挙動、拡散、権限昇格、セーフモード、運用上のカスタマイズに関するオプションが含まれます。具体的な引数はバリアントごとに異なります（前部参照）。 T1059.001 - コマンドおよびスクリプトインタープリタ：PowerShell（Command and Scripting Interpreter: PowerShell） ネットワーク共有接続を変更した後、LanmanWorkstationサービスを再起動するためにPowerShellコマンドを実行します。また、PowerShellおよびActive Directoryコマンドを用いてサービスの再起動やドメイン内コンピュータの列挙を行います。さらに、-kill-clusterオプションによりVMクラスタを停止し、-spread-vcenterオプションにより提供された認証情報とパイナリを使用してvCenter/ESXi環境内で拡散する機能も備えています。 T1569.002 - システムサービス：サービス実行（System Services: Service Execution） 新しいAgendaのRustバリアントは、リモートでのサービス実行のためにPsExecを内蔵しています。-propagateまたは-spreadオプションで実行された場合、マルウェアはPsExecを%UserTemp%ディレクトリに配置し、それを用いてリモートホスト上でマルウェアを実行します。 T1569.002 - システムサービス：サービス実行（System Services: Service Execution） 本ランサムウェアは「truesight」という名前のTrueSightKillerサービスを作成するか、既存の場合はそれを起動します。また、ランダムな名前で%Zemana Anti-Malwareドライバを%System%\drivers\配下に配置し、HKLM\SYSTEM\CurrentControlSet\Servicesに対応するサービスエントリを作成してSpyboyドライバを読み込ませます。 T1129 - 共有モジュール（Shared Modules） TrueSightKiller（Truesight.sys）およびRogueKiller Antirootkit Driverを使用しており、これらはいずれもAdlice製品スイートの一部です。	T1547.001 - ブートまたはログオン時の自動実行：レジストリRunキー／スタートアップフォルダ（Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder） 本ランサムウェアは、runonceの自動起動レジストリエントリを作成します。 T1543.003 - システムプロセスの作成または変更：Windowsサービス（Create or Modify System Process: Windows Service） wmicおよびnetコマンドを使用してVSSサービスを変更および無効化し、シャドウコピーの作成を阻止します。 T1547.001 - ブートまたはログオン時の自動実行：レジストリRunキー／スタートアップフォルダ（Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder） レジストリ内のImagePath値を変更し、システム起動時に実行ファイルが確実に起動されるようにして、Persistence-as-a-Service（PaaS）としての永続化を実現します。 T1053 - スケジュールされたタスク／ジョブ（Scheduled Task/Job） 特定のキャンペーンでは、「veeamupdate」という名前のスケジュールタスクを作成し、システム侵害後にランサムウェアのバイナリを実行するよう設定されていることが確認されています。	T1134.001 - アクセストークン操作：トークンのなりすまし／窃取（Access Token Manipulation: Token Impersonation/Theft） 本ランサムウェアは設定からアカウント情報を取得してログインを試行し、取得したユーデートークンを使用して、CreateProcessAsUserを介し「-alter {ポート番号}」引数付きでプロセスを作成します。 T1055 - プロセスインジェクション（Process Injection） その後、改変されたDLL（pwndll.dll）をPublicフォルダに配置し、svchost.exeにインジェクションすることで、ランサムウェアバイナリの継続的な実行を可能にします。 T1484.001 - ドメインまたはテナントポリシーの変更：グループポリシーの改変（Domain or Tenant Policy Modification: Group Policy Modification） 特定のキャンペーンでは、エンドポイントのホスト名をドメインコントローラ名として管理共有に使用し、悪意のあるGPO変更を適用することで、さらなる不正動作を有効化することが確認されています。 T1078 - 有効なアカウント：ローカルアカウント（Valid Accounts: Local Accounts） 特定のキャンペーンでは、「Support」という名称のバックドア管理者アカウントを作成し、net.userおよびnet localgroupコマンドを用いて、永続的な特権アクセスを維持することが確認されています。 T1098 - アカウント操作（Account Manipulation） 特定のキャンペーンでは、正規のAdministratorアカウントのパスワードをリセットし、net user Administrator *****コマンドを用いて管理権限を維持するとともに、正規管理者によるアクセス回復を妨害する動きが確認されています。

横展開	情報送出	コマンド＆コントロール	認証情報の取得
T1021 - リモートサービス：リモートデスクトッププロトコル（Remote Services: Remote Desktop Protocol） Agendaランサムウェアは、reg addコマンドでレジストリを変更することでリモートデスクトップ接続を有効化します。また、netshによるファイアウォール設定の変更やレジストリキーの調整によってRDPセッションを許可します。さらに、ネットワーク共有にプログラムを書き込み、PsExecを使用してリモートシステム上でコマンドを実行します。加えて、SMBやWindows管理共有を利用してCobalt Strikeにより追加のペイロードを展開し、ラテラルムーブメントを実行します。 T1021 - リモートサービス：SMB／Windows管理共有（Remote Services: SMB/Windows Admin Shares） 管理共有を利用して、ネットワーク上のエンドポイント間でマルウェアを拡散します。 T1021.004 - リモートサービス：SSH（Remote Services: SSH） ファイル転送のためにSSHを有効化し、SSHセッションを確立してターゲットホストにペイロードをアップロードおよび実行した後、切断します。その後、PuTTYを使用してSSH接続を確立し、認証情報の窃取やフィッシングによって取得した正規のSSH認証情報を利用して、侵害ネットワーク内でラテラルムーブメントを行います。	T1567.002 - クラウドストレージへのデータ持ち出し（Exfiltration to Cloud Storage） 過去のAgendaランサムウェアのキャンペーンでは、クラウド同期サービスであるMEGAsyncを使用して、クライアントからリモートのクラウドサーバへファイルを持ち出していたことが確認されています。また、収集した情報はHTTP POSTを通じて送信されます。 T1567.002 - Webサービス経由のデータ持ち出し：クラウドストレージ（Exfiltration Over Web Service: Exfiltration to Cloud Storage） Agendaランサムウェアは、WinSCPを使用して被害環境からファイルを持ち出します。また、s3cmdツールを使用し、認証情報を用いて機密文書、メール、データベースファイルなどを選択的にクラウドオブジェクトストレージへ送信します。 T1041 - C2チャネル経由のデータ持ち出し（Exfiltration Over C2 Channel） Coroxy/SystemBCを使用して被害者のユーザー名をGetUserNameExAで取得し、RC4で暗号化して通信中の秘匿性を確保した上で、初期登録の一部としてC&Cサーバへ送信します。	T1071 - アプリケーション層プロトコル：Webプロトコル（Application Layer Protocol: Web Protocols） C&Cサーバとの通信において、直接的なTCP接続、プロキシチャネル、HTTP/HTTPS（Coroxy/SystemBC、SmokeLoader、Mongoose Web Server）を使用します。また、MeshAgentを悪用し、WebSocket（wss://）を介してMeshCentralのC&Cサーバ（agent.ashx）へ接続します。 T1090 - プロキシ：外部プロキシ（Proxy: External Proxy） Coroxy/SystemBCを使用してプロキシチャネルを確立し、暗号化された通信を中継するとともに、セッション終了時にC&Cサーバへ通知します。 T1105 - ツールの転送（Ingress Tool Transfer） 攻撃者からさまざまなペイロードを受信して実行し、その実行挙動はペイロードの種類に依存します。また、MeshAgentを悪用してWindowsホスト上でLinux用ランサムウェアバイナリを転送および実行します。 T1188 - マルチホッププロキシ（Multi-hop Proxy） Torを使用してC&C通信を中継します。 T1219 - リモートアクセスツール（Remote Access Tools） RemotelyやMeshCentralといった正規のリモートアクセスツールを利用し、侵害されたシステムへの持続的なアクセスおよび制御を維持します。	T1081 - ファイル内の認証情報（Credentials in Files） Veeamバックアップデータベースの「Credentialsテーブル」に対して「SELECT [user_name], [password] FROM [VeeamBackup].[dbo].[Credentials]」というクエリを実行し、保存されているユーザー名およびパスワードを抽出します。

探索	検出回避	影響
T1057 - プロセスの探索（Process Discovery） Agendaランサムウェアは、終了対象となる特定のプロセスを検出します。また、OS種別（Linux、Nutanix、VMKernel、FreeBSD、ESXi、Unknown）、CPU数、OSバージョン、ベンダーID、プロセッサ情報、メモリ情報などのシステム情報を収集します。 T1135 - ネットワーク共有の探索（Network Share Discovery） NetShareEnumを使用してネットワーク共有を列挙し、ネットワーク上での暗号化活動に利用します。 T1082 - システム情報の探索（System Information Discovery） OS種別（Linux、VMKernel、FreeBSD、ESXi、Unknown）、CPU数、OSバージョン、ベンダーID、プロセッサ情報、メモリ情報などのシステム情報を収集します。また、対象システムにインストールされている製品を列挙するコマンドも実行します。 T1083 - ファイルおよびディレクトリの探索（File and Directory Discovery） システム内のファイルを列挙して暗号化対象となるファイルを特定し、特定の文字列や拡張子を持つファイルは暗号化対象から除外します。 T1033 - システム所有者／ユーザーの探索（System Owner/User Discovery） PowerShellコマンドを使用してActive Directory上のコンピューター覧を取得し、自身をそれらにコピーします。また、whoami /groupsコマンドでユーザーのグループ情報を取得し、query sessionコマンドでアクティブなセッションを列挙します。 T1087.001 - アカウント探索：ローカルアカウント（Account Discovery: Local Account） 2024年2月に観測されたRust版は、PowerShellによる拡散スクリプトを使用して、対象マシン上のESXiホストを列挙します。 T1087 - アカウント探索：ドメインアカウント（Account Discovery: Domain Account） 過去のAgendaキャンペーンでは、PC Hunter中net groupコマンドを使用して、Domain AdminおよびEnterprise Adminグループの情報を収集していたことが確認されています。 T1087.002 - アカウント探索：ドメインアカウント（Account Discovery: Domain Account） net groupコマンドを使用して、Domain AdminsおよびEnterprise Adminsグループのメンバーを取得します。 T1018 - リモートシステムの探索（Remote System Discovery） 特にドメインコントローラなどのリモートシステムを検出し、nltestコマンドを使用して指定ドメイン内のすべてのドメインコントローラを列挙します。 T1049 - システムネットワーク接続の探索（System Network Connections Discovery） WannaMine、PC Hunter、YDArkPassなどのツールを使用してポートスキャンを実施し、TCP接続の一覧取得、ポートおよびT4444で動作するプロセスの確認、現在のネットワーク接続状況の把握を行います。 T1046 - ネットワークサービスの探索（Network Service Discovery） HRSwordツールを使用し、NetShareEnum APIを介してネットワーク共有を列挙し、ネットワーク暗号化の処理に利用します。 T1010 - アプリケーションウィンドウの探索（Application Window Discovery） SmokeLoaderを使用し、ウィンドウクラス名を特定することで特定のプロセスを識別し、終了させます。	T1562 - 防御の無効化（Impair Defenses） Agendaランサムウェアは、検出や防御を回避するためにアンチウイルス関連のサービスやプロセスを終了させます。また、実行中のプロセスを継続的にスキャンし、eskle.sysドライバに対してDeviceIoControlを通じて終了コマンドを送信し、対象プロセス名を指定して停止させます。 T1562.001 - 防御の無効化：ツールの無効化または変更（Disable or Modify Tools） ユーザーアカウント制御（UAC）を無効化し、管理者権限の要求プロンプトを抑止することで、システム保護を低下させます。 T1480 - 実行ガードレール（Execution Guardrails） 実行前に、保存されたハッシュと照合して検証されるパスワードキーの入力を要求します。 T1070.001 - 痕跡の削除：Windowsイベントログのクリア（Indicator Removal: Clear Windows Event Logs） wevtutilおよびPowerShellを用いてコマンドを実行し、すべてのWindowsイベントログを削除してフォレンジック痕跡を消去します。 T1222.001 - ファイルおよびディレクトリ権限の変更：Windows（Windows File and Directory Permissions Modification） fsutilコマンドを使用してシンボリックリンクの評価設定を変更し、侵害されたネットワーク内でファイルシステムアクセスを別の場所へリダイレクトします。 T1562.009 - 防御の無効化：セーフモード起動（Safe Mode Boot） -safe引数で実行された場合、bcdedit /set {current} safeboot networkを用いて、ネットワーク付きセーフモードでシステムを再起動するプロセスを追加します。 T1070.004 - 痕跡の削除：ファイル削除（Indicator Removal: File Deletion） -no-deleteが指定されていない場合、cmd /C timeout /T 5 & Del:コマンドを使用して実行後に自身を削除します。2024年2月に観測されたバージョンでは、-no-destructが指定された場合に自己削除を回避します。 T1497.001 - 仮想化／サンドボックス回避：システムチェック（Virtualization/Sandbox Evasion: System Checks） CPUIDチェックにより実行環境を識別し、-no-vmが指定されていない場合は仮想マシンを終了させることがあります。また、-no-sandboxが指定されていない場合はサンドボックス環境を模知します。さらに、System\CurrentControlSet\Enum\IDEおよびSystem\CurrentControlSet\Enum\SCSI配下のレジストリサブキーを列挙して仮想化に関連する文字列を検出し、該当した場合は終了します。加えて、メモリ内にSbiedllモジュールが読み込まれているかも確認します。 T1134.005 - アクセストークン操作：SID履歴インジェクション（Access Token Manipulation: SID-History Injection） -escalated -parent-sid {SID}で実行された場合、指定されたSIDのコンテキストで動作することが可能です。 T1497.003 - 仮想化／サンドボックス回避：時間ベース回避（Time Based Evasion） -timerが指定された場合、指定された時間だけ実行を遅延させます。 T1564 - 痕跡の隠蔽（Hide Artifacts） 2024年2月に観測されたRust版のAgendaランサムウェアは、拡散スクリプト内でVMware PowerCLIモジュールを改変し、実行失敗時のエラープロンプトを抑制します。 T1222.002 - ファイルおよびディレクトリ権限の変更：LinuxおよびMac（Linux and Mac File and Directory Permissions Modification） 2024年2月に観測されたRust版は、拡散スクリプト内でchmodを使用し、コピーしたファイルの権限を変更して実行可能にします。 T1140 - ファイルまたは情報の難読化解除／デコード（Deobfuscate/Decode Files or Information） 2024年2月に観測されたRust版は、.NETローダーを使用してアセンブリを復号・動的ロードし、その型を反復処理してリフレクション経由で難読化されたメソッドを実行します。 T1027.002 - 難読化されたファイルまたは情報：ソフトウェアパッキング（Obfuscated Files or Information: Software Packing） 2024年11月に観測された後期バージョンでは、.NET Reactor v6でパックされたNETXLOADERにより、プロセスインジェクションを通じて読み込まれていることが確認されています。 T1055.002 - プロセスインジェクション：ポータブル実行形式（Portable Executable Injection） 2024年11月に観測されたRust版には、VirtualAllocでメモリを確保し、ペイロードをコピーした後、VirtualProtectでメモリ保護をPAGE_EXECUTE_READWRITEに変更し、CreateThreadでスレッドを生成してペイロードを実行し、WaitForSingleObjectで終了を待機するローダーが含まれています。 T1553.002 - 信頼制御の回避：コード署名（Subvert Trust Controls: Code Signing） KAPROCHANDLERを使用した署名済みドライバを悪用し、アンチウイルス製品に関連するファイルの削除やプロセスの終了を行います。	T1490 - システム回復の妨害（Inhibit System Recovery） vssadmin delete shadows /all /quietコマンドを使用してシャドウコピーを削除します。新しいRust版のAgendaランサムウェアでは、cipher /w:{ドライブレター}:\ を使用して削除済みデータを上書きします。 T1486 - 影響を与えるためのデータ暗号化（Data Encrypted for Impact） 初期のAgendaランサムウェアは、-n、-p、fast、skip、stepなどのフラグを用いた間欠的暗号化に対応していました。2024年6月に観測されたバージョンでは、no-mountedによりマウントされていない共有をスキップし、no-priorityにより特定ファイルの優先処理を回避します。 Agendaランサムウェアはrand_read()を用いてAES-256の暗号鍵とIVを生成し、ファイルをAES-256で暗号化した後、組み込みの公開鍵を使用してRSA-2048で鍵を暗号化します。また、引数やフラグに応じた間欠的暗号化もサポートしています。 Linux版のAgendaランサムウェアは、RSAとAESを使用したファイル暗号化を行い、マルチスレッド処理に対応し、設定されたステップサイズに基づく間欠的暗号化を実行します。 T1489 - サービス停止（Service Stop） サービスを終了させ、無効化します。 T1491.001 - 改ざん：内部改ざん（Defacement: Internal Defacement） 実行後にレジストリを変更して壁紙を変更し、さらにmotdファイルを改変してユーザーログイン時にランサムノートを表示させます（前部参照）。 T1531 - アカウントアクセスの削除（Account Access Removal） Rust版のAgendaランサムウェアは、侵入したvCenterおよびESXiホストのrootパスワードを、ランサムウェア実行時のパスワードに変更します。2024年6月に観測されたバージョンでは、-safeで実行された場合にパスワード変更を通じてユーザーアクセスを削除する機能があります。 T1561.001 - ディスクワイプ：ディスク内容の消去（Disk Wipe: Disk Content Wipe） ESXiデバイス上のVMFS-5およびVMFS-6の仮想ディスクを削除し、仮想マシン上で実行された場合にはスナップショットも削除します。 T1496 - リソースの乗っ取り（Resource Hijacking） 初期のAgendaキャンペーンでは、コインマイナーのファイルをダウンロードしていたことが確認されています。