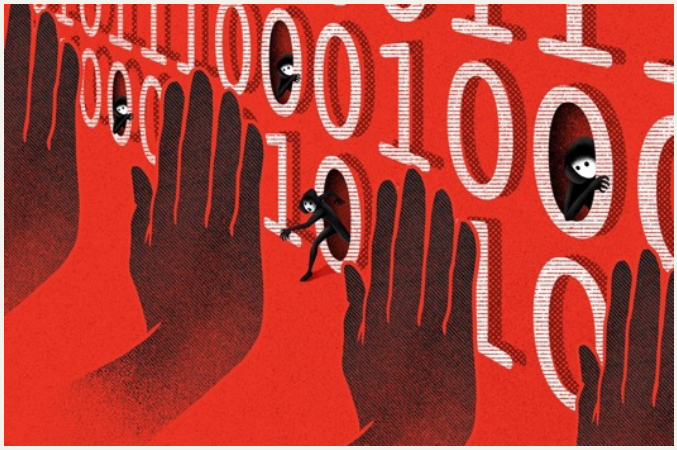
ランサムウェアの進化は企業を悩ませていますが、CrowdStrikeの保護機能は決して揺らぎません。

November 11, 2021 | Thomas Moses | Sarang Sonawane | Liviu Arsene | エンドポイント & クラウドセキュリティ

- サイバー犯罪活動の脅威が蔓延する中、ランサムウェアはその大きな原因に
- ランサムウェアを使う攻撃者は、コードとその効果を常に改善し続けている
- CrowdStrikeの改良された振る舞い検知機能が、ランサムウェアによるボリュームシャドウコピーの改ざんを防止
- ボリュームシャドウコピーサービス（VSS）のバックアップ保護機能により、攻撃者による削除の試行を無効化し、スナップショットを復元可能な状態に維持



サイバー犯罪の世界における**ランサムウェア**の影響は大きく、大きな混乱を引き起こすランサムウェアは企業にとっての大きな懸念材料になっています。最新の **CrowdStrike 2021 年版脅威ハンティングレポート**によれば、2020 年 7 月から 2021 年 7 月にかけて発生したインタラクティブ型（対話型）の侵入活動のうち、サイバー犯罪は 75% 以上を占めています。絶えず進化するビッグゲームハンティング（BGH）のビジネスモデルは、アクセスを容易にするアクセスブローカーで広く採用されています。その主な原動力は、被害者のコンプライアンスに圧力をかけるための専用リークサイトです。ランサムウェアは絶えず進化しており、また脅威アクターは、被害者によるデータ復元をより困難にするコンポーネントや機能を実装しています。

Lockbit 2.0 の人気

正規の vssadmin.exe Windows ツールを悪用して Microsoft Server ボリュームシャドウコピーサービス（VSS）を改ざんするなど、LockBit ランサムウェアの能力はますます強化されています。ランサムウェアを駆使する攻撃者が広く用いる効果的な戦術には、**ラテラルムーブメント**の能力や、シャドウコピーを破壊する能力などもあります。

図 1　LockBit 2.0 ランサムのメモ（クリックして拡大）

LockBit 2.0 ランサムウェアは他のランサムウェアと類似する能力を持っており、これには、UAC（ユーザーアカウント制御）を迂回する能力や、被害者のシステム言語を暗号化前に確認してロシア語圏の国にないことを確認したり、自己終了する能力などがあ

ります。

たとえば LockBit 2.0 は、GetSystemDefaultUILanguage と GetUserDefaultUILanguage の Windows API 呼び出しを使用して、システムのデフォルト言語と現在のユーザーを確認し、言語コード識別子が指定されたものと一致する場合は、プログラムを終了します。図 2 は、どのように言語検証が行われるかを示しています（関数呼び出し 49B1C0）。

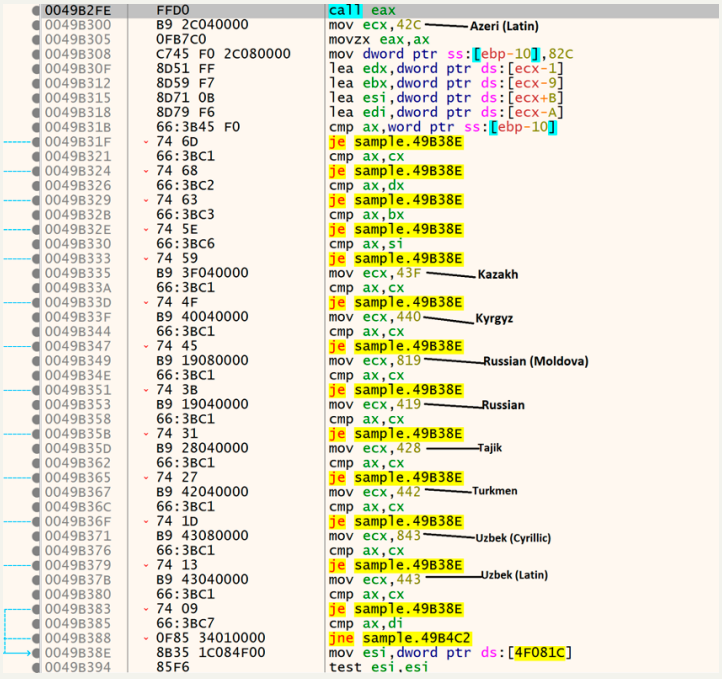


図 2　システム言語チェックを実行する LockBit 2.0

また LockBit は、アラートや UAC ポップアップをトリガーさせずに、UAC をサイレントに迂回して暗号化を実行することもできます。LockBit はまず、LockBit が管理者特権で実行されているかを確認します。この確認は、API 関数を使用してプロセストークンを取得し（NTOpenProcessToken）、SID 識別子を生成して権限レベルを確認し（CreateWellKnownSid）、現在のプロセスに十分な管理者特権があるかを確認することで行われます（CheckTokenMembership および ZwQueryInformationToken 関数）。

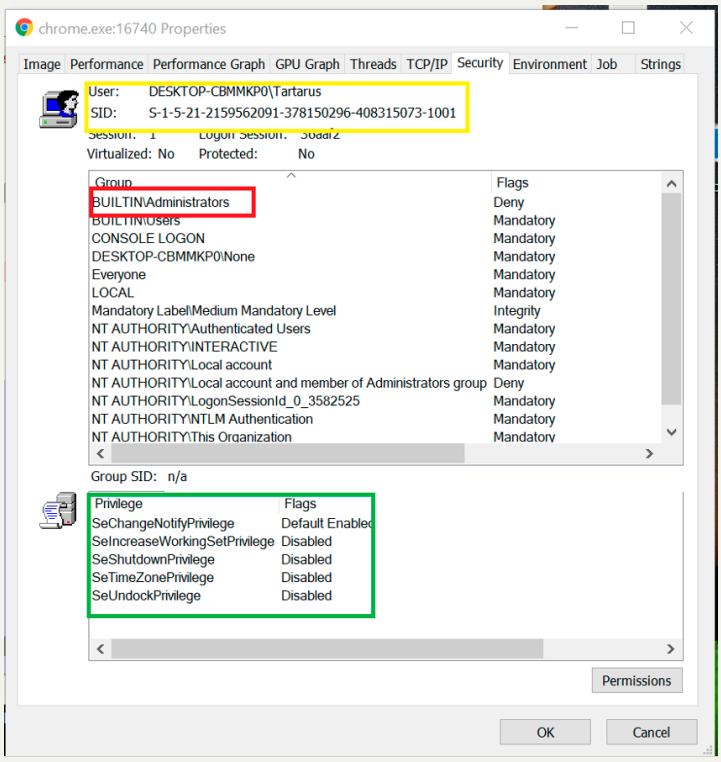


図 3 プロセス実行の SID 権限グループ

プロセスが管理者特権で実行されていない場合、LockBit は、guid 付きの elevation moniker COM 初期化メソッドを利用して、COM インターフェースの昇格により COM オブジェクトを初期化して管理者特権での実行を試みます（Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}）。同様の昇格手法は、DarkSide ランサムウェアや REvil ランサムウェアでも過去に使用されています。

LockBit 2.0 はラテラルムーブメントする能力も有しており、他のホストをスキャンして他のネットワークマシンに拡散できます。たとえば、LockBit 2.0 は GetLogicalDrives 関数を呼び出して、現在利用可能なドライブのビットマスクを取得し、システムで利用可能なドライブを一覧表示します。特定されたドライブがネットワーク共有の場合、LockBit 2.0 はそのリソースの名前を特定して、WNetGetConnectionW、PathRemoveBackslashW、OpenThreadToken、DuplicateToken などの API 関数で接続を試みます。

つまり、個々のマシンを標的にして侵害するのではなく、ネットワーク全体を侵害するということです。**REvil** や LockBit は、まさにこの機能を持つ最近のランサムウェアファミリーの一例であり、**Ryuk** や WastedLocker などにも同様の機能があります。CrowdStrike Falcon OverWatch™ チームは、侵入の 36% がラテラルムーブメント能力を持っていて、30 分以内に他のホストに展開できると **CrowdStrike 2021 年版脅威ハンティングレポート**で報告しています。

また LockBit 2.0 は、データの暗号化能力や抽出能力の他に、身代金に関するメモメッセージをネットワークに接続されたすべてのプリンタでプリントアウトし、被害者を公に辱める機能も有しています。

VSS 改ざん：確立されたランサムウェアの戦術

VSS シャドウコピーの改ざんや削除はよく使用される戦術であり、これによりデータ復旧が困難になります。攻撃者は正規の Microsoft 管理ツールを悪用して VSS シャドウコピーの無効化、削除を実行することがよくあります。使用されるツールには、Windows Management Instrumentation（WMI）、BCDEdit（ブート構成データの管理に使用されるコマンドラインツール）、vssadmin.exe などが見られます。LockBit 2.0 は以下の WMI コマンドラインを利用して、シャドウコピーを削除します。

```
C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
```

WMI などのインストール済みのオペレーティングシステムツールが使用されることは昔からありました。今でも攻撃者は、侵害されたシステム上で悪意のある実行ファイルを実行したり、ディスクに書き込む代わりに、このようなツールを初期アクセスの手段として用いています。また、2021 年 4 月から 6 月に検知された攻撃のうち、68% がマルウェアフリーであることが **CrowdStrike Threat Graph®** で明らかになっています。攻撃者は、自律検知を回避するようカスタマイズされた、より洗練されたステルス手法や、マルウェアを超えた手法を実践しています。

CrowdStrike で VSS を保護する

CrowdStrike Falcon は、多層防御の手法により、振る舞いベースの**攻撃の痕跡（IOA）**や高度な機械学習などの機能を活用して、ランサムウェアの検知、予防を実現します。CrowdStrike は、既知および未知の脅威や攻撃者に対抗する CrowdStrike テクノロジーの効果を改善し続けています。

CrowdStrike の強化された IOA 検知能力は、悪意のある振る舞いとそうでないものを正確に識別し、信頼性の高い検知結果を実現できます。この機能は、バックアップソリューションなどの正当なソフトウェアと似た能力をランサムウェアが有している場合に、特に重要になります。どちらも、ディレクトリを列挙して一見重要ではないファイルを書き込む機能を持ちますが、エンドポイント上の他の痕跡と関連付けることで、本物の攻撃を特定することができます。一見通常である振る舞いを相互に関連付けることで、さまざまなマルウェアを幅広く特定することができるようになります。たとえば、単一の IOA だけで、複数のファミリーに加えて未知のファミリーもカバーできます。

また、CrowdStrike に最近追加された機能としてシャドウコピーを改ざんから保護する機能があり、ランサムウェア攻撃を軽減する保護レイヤーを追加することでこれを実現しています。シャドウコピーを保護することで、侵害の危険性のあるシステムで暗号化されたデータをはるかに少ない時間と労力で復元できるようになります。最終的に、侵害され暗号化されたシステムの起動に使われる人間の時間的労力が削減されるため、運用コストの削減につながります。

Falcon プラットフォームでは、疑わしいプロセスがシャドウコピーを改ざんしたり、ファイルサイズを変更してバックアップを無効にするなどのアクションを防止できます。たとえば、LockBit 2.0 ランサムウェアの感染が発生し、正当な Microsoft 管理ツール（vssadmin.exe）を使用してシャドウコピーを操作しようとする試行が行われると、Falcon は即座にこの振る舞いを検知し、ランサムウェアによる削除や改ざんを防止します（図 4 を参照）。

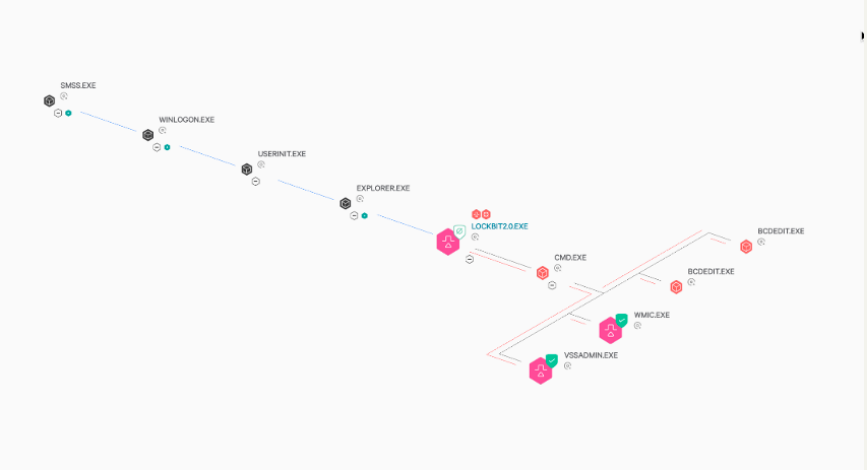


図 4　LockBit 2.0 ランサムウェアによる vssadmin.exe の悪用を検知してブロックする Falcon（クリックして拡大）

つまり、ランサムウェア感染で侵害されたエンドポイント上のファイルが暗号化される可能性があったとしても、Falcon によりシャドウコピーの改ざんは防止されるため、企業側のデータ復元が容易になります。

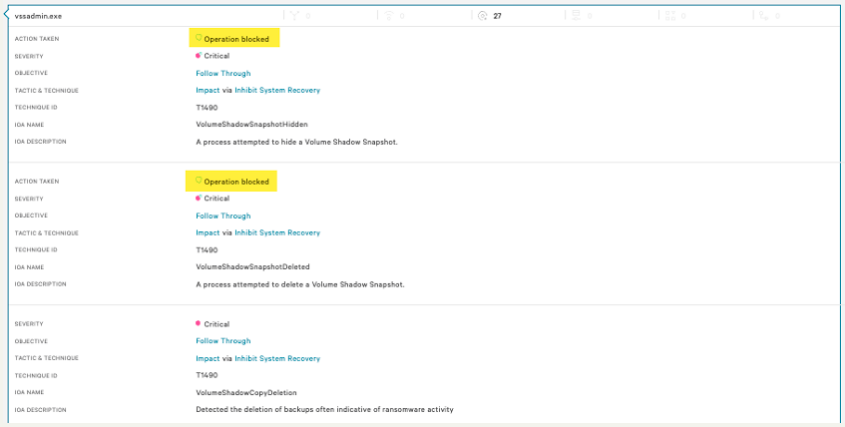
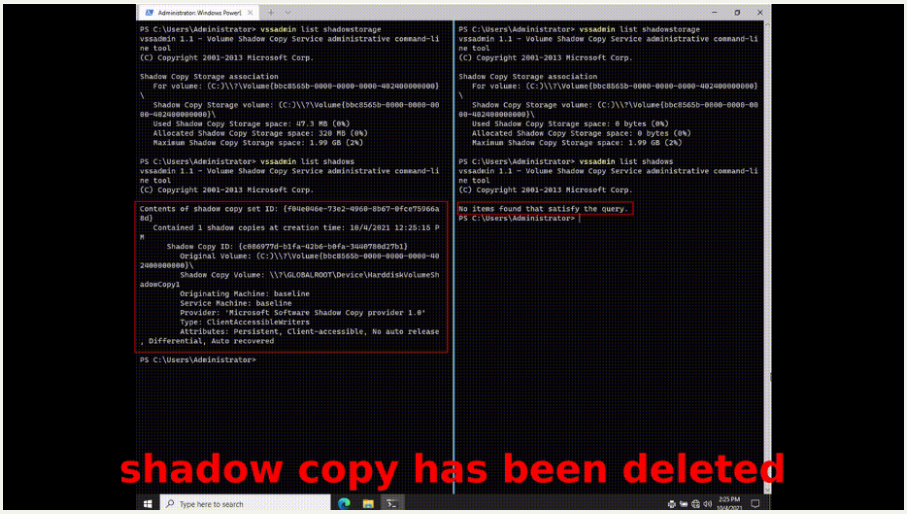


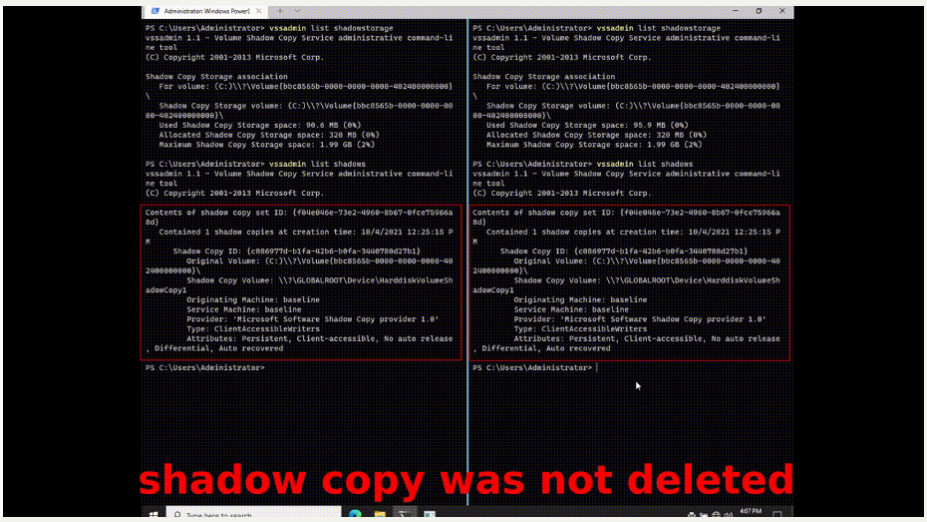
図 5　VSS シャドウコピーの削除を試みる、検知、ブロックされたランサムウェアのアクティビティに対する Falcon アラート（クリックして拡大）

以下は、Falcon の保護がないシステムで実行される Lockbit 2.0 です。ここでは、シャドウコピーの一覧表示に vssadmin が使用されています。実行後、シャドウコピーが削除されていることに注目してください。



（クリックして動画を表示）

以下でも同じ Lockbit 2.0 が実行されていますが、こちらの場合は Falcon と VSS 保護が有効になっています。ランサムウェアが正常に実行されたにもかかわらず、シャドウコピーは削除されていません。また、このデモンストレーションでは、このランサムウェアの実行をあえて許可して行っています。



（クリックして動画を表示）

CrowdStrike は、ボリュームシャドウサービスバックアップ保護でシャドウコピーの破壊や改ざんを防止します。また、脅威アクターが使う手法が従来型か最新かによらず、復元可能な状態のスナップショットを保持できます。ライブシステムは、ダイレクトスナップショットツールやシステム復元を使用して、攻撃後に即座に復元できます。

VSS シャドウコピー保護の機能は、CrowdStrike の多層防御に新たに追加された改善のひとつに過ぎません。CrowdStrike は、侵害を防止するという使命に取り組み続けています。また、機械学習と振る舞いベースの検知、保護機能を継続的に改善することで、Falcon プラットフォームが高度な攻撃者や脅威に関連する戦術、技術、手順を検知して保護できるようにしています。

CrowdStrike の多層防御でクラス最高の保護を実現

Falcon プラットフォームではインテリジェンス、テクノロジー、専門性を統合することで、ランサムウェアを正常に検知して保護します。毎週数兆単位で発生するイベントからなる大量のデータセットと、脅威アクターのインテリジェンスで強化された人工知能（AI）ベースの機械学習、および IOA の振る舞いによりランサムウェアを検知してブロックします。ステルス攻撃さえもプロアクティブに特定し防止する脅威ハンティングのエキスパート、および Falcon プラットフォームの多層防御アプローチで、企業にとって最も重要なものをランサムウェアなどの脅威から保護できます。

CrowdStrike **Falcon のエンドポイント保護パッケージ**では、正常に侵害を止めるために必要となる包括的テクノロジー、インテリジェンス、専門知識がひとまとめにされています。フルマネージドの検知と対応（MDR）を可能とする Falcon Complete™ の経験豊富なセキュリティ専門家が、**403% の ROI と 100% の信頼性**を実現します。

侵害の痕跡（IOC）

ファイル	SHA256
LockBit 2.0	0545f842cazz2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049

原文：Ransomware (R)evolution Plagues Organizations, But CrowdStrike Protection Never Wavers
https://www.crowdstrike.com/blog/how-crowdstrike-prevents-volume-shadow-tampering-by-lockbit-ransomware/