

初期侵入	不正活動の実行	検出回避	クレデンシャルアクセス	事前調査	水平移動・内部活動	情報送出	被害規模
T1078 - 有効なアカウント トレンドマイクロではランサムウェア BlackCat の攻撃者が漏えいしたアカウント情報を使用して被害者のネットワークにアクセスすることを確認しています。	T1059 - コマンドおよびスクリプトのインタープリタ ランサムウェア BlackCat のバインナリは、不正活動を続けるために正規のアクセストークンを必要とします。 また、異なる追加機能に使用される他の引数も受け付けません。	T1562.001 - 防御機能の無効：ツールの無効化または変更 トレンドマイクロでは、攻撃者が ConnectWise とコマンドラインを使用して、セキュリティ対策ソフトをアンインストールすることで、被害者のネットワークへの足場を固めることを確認しています。	T1003.001 - OS クレデンシャルダンプ：LSASS メモリ 攻撃者は、Process Hacker を使用して、lsass.exe のメモリをダンプします。	T1087 - アカウントの探索 ランサムウェアは、さまざまなツールを使用してアカウント情報を収集します。 T1083 - ファイルとディレクトリの探索 ランサムウェアは、暗号化のためのファイルとディスカバリーを探索します。	T1021.002 - リモートサービス：SMB / Windows 管理者共有 このランサムウェアには、他のリモートホストに自身を拡散させる際に使用する PsExec モジュールが埋め込まれています。また、API NetShareEnum を使用してネットワーク共有を列挙します。	T1048 - 代替プロトコルによる情報送出 ExMatter と FileZilla を使用し、代替プロトコルを介して窃取情報を送出します。	T1489 - サービス停止 さまざまなサービスを終了します。 T1490 - システム回復の禁止 シャドウ コピーを削除してシステム回復を無効にします。
T1190 - 公開アプリケーションの脆弱性悪用: 以下の MS Exchange サーバの脆弱性を介して侵入します。 - CVE-2021-26855 - CVE-2021-26857 - CVE-2021-26857 - CVE-2021-27065	T1059 - コマンドおよびスクリプトのインタープリタ ランサムウェア BlackCat のバインナリは、不正活動を続けるために正規のアクセストークンを必要とします。 また、異なる追加機能に使用される他の引数も受け付けません。	T1562.009 - 防御機能の無効：セーフモードを起動する ランサムウェア BlackCat のバインナリは、影響を受けるシステムを再起動する前にセーフモードで自動実行できるように、自身をサービスとして登録する機能を備えています。	T1003.001 - OS クレデンシャルダンプ：LSASS メモリ 攻撃者は、Process Hacker を使用して、lsass.exe のメモリをダンプします。	T1057 - プロセスの探索 ランサムウェアは、終了対象となるプロセスを探索します。 T1135 - ネットワーク共有の探索 ランサムウェアは、さまざまなツールを使用してアカウント情報を収集します。		T1567 - ウェブサービスを介した情報送出 ExMatter、Rclone、MEGASync、WinSCP などの Web サービスを介して窃取情報を送出します。	T1486 - 情報の暗号化による被害をもたらす ランサムウェアのペイロードは、ファイルを暗号化し、自身の構成内の拡張子を追加します。 T1491.001 - 改ざん：内容の改ざん ランサムウェアのペイロードは、感染端末の壁紙イメージを変更します。
		T1070.001 - ホスト上のインジケータの削除：Windows イベントログの消去 ランサムウェア BlackCat のバインナリは、wevtutil.exe を使用して、被害を受けた企業や組織の Windows イベントログを消去します。	T1003.001 - OS クレデンシャルダンプ：LSASS メモリ 攻撃者は、Process Hacker を使用して、lsass.exe のメモリをダンプします。	T1016 - システムネットワーク構成の探索 ランサムウェアは、さまざまなツールを使用してアカウント情報を収集します。 T1069 - グループ権限の探索 ランサムウェアは、さまざまなツールを使用してアカウント情報を収集します。 T1018 - リモートシステムの検出 ランサムウェアは、さまざまなツールを使用してアカウント情報を収集します。			