戦略 （Tactics）	技術 （Techniques）	ID	本攻撃との関わり
初期アクセス （Initial Access）	サプライチェーン侵害：ソフトウェアのサプライチェーン （Supply Chain Compromise: Compromise Software Supply Chain）	T1195.002	両事例：Docker Hubイメージ、VS Code拡張機能、PyPIパッケージ、GitHub Actionsを侵害
初期アクセス （Initial Access）	有効なアカウント （Valid Accounts）	T1078	KICS事例：Docker Hub、VS Code、GitHub Actionパブリッシャーの認証情報を利用して不正なバージョンを配布
初期アクセス （Initial Access）	信頼関係 （Trusted Relationship）	T1199	elementary-data事例：プルリクエスト・コメントへのインジェクションにより、GitHub Actionsランナーのトークンを悪用
実行 （Execution）	コマンドやスクリプトのインタプリタ：JavaScript （Command and Scripting Interpreter: JavaScript）	T1059.007	KICS事例：被害システム上でBunランタイムを通してmcpAddon.jsを実行
実行 （Execution）	コマンドやスクリプトのインタプリタ：Python （Command and Scripting Interpreter: Python）	T1059.006	elementary-data事例：Pythonインタプリタの開始時に「.pth」のペイロードを実行
実行 （Execution）	コマンドやスクリプトのインタプリタ：Unixシェル （Command and Scripting Interpreter: Unix Shell）	T1059.004	elementary-data事例：コメントインジェクション後、GitHub Actionsのランナーがシェル・ステージャを実行
永続化 （Persistence）	起動/ログオン時の自動起動 （Boot or Logon Autostart Execution）	T1547	elementary-data事例：ホスト上でPythonインタプリタが起動するたびに「.pthファイル」を実行
防御回避 （Defense Evasion）	ファイルやデータの難読化 （Obfuscated Files or Information）	T1027	KICS事例：「AES-256-GCM」と「RSA OAEP-SHA256」で暗号化 elementary-data事例：「MD5キーストリーム」によるXOR暗号化
防御回避 （Defense Evasion）	痕跡の消去：ファイル削除 （Indicator Removal: File Deletion）	T1070.004	elementary-data事例：一時ディレクトリのコンテキストマネージャを利用し、処理の完了時にファイル「trin.tar.gz」を削除
認証情報アクセス （Credential Access）	安全でない認証情報：ファイル内に保存された認証情報 （Unsecured Credentials: Credentials In Files）	T1552.001	両事例：SSH鍵、クラウド上の認証情報ファイル、ディスク内の開発者トークンを収集
認証情報アクセス （Credential Access）	安全でない認証情報：クラウドインスタンスのメタデータAPI （Unsecured Credentials: Cloud Instance Metadata API）	T1552.005	elementary-data事例：スティーラーが「EC2 IMDS v2」や「ECSタスクの認証情報エンドポイント」に問い合わせを実行
認証情報アクセス （Credential Access）	アプリケーションのアクセストークンを窃取 （Steal Application Access Token）	T1528	elementary-data事例：GitHub Actionsランナー上のトークン「GITHUB_TOKEN」を悪用してリリースコミットを偽造
探索 （Discovery）	クラウドサービスの探索 （Cloud Service Discovery）	T1526	elementary-data事例：API「secretsmanager:ListSecrets」や「ssm:DescribeParameters」をその場で呼び出して探索実行
探索 （Discovery）	コンテナやリソースの探索 （Container and Resource Discovery）	T1613	elementary-data事例：コマンド「kubectl get secrets --all-namespaces」を用いて探索実行

情報収集 （Collection）	ローカルシステムからの情報収集 （Data from Local System）	T1005	認証情報ファイル、シェル履歴、AI/MCP設定ファイルを収集
情報収集 （Collection）	クラウドストレージからの情報収集 （Data from Cloud Storage）	T1530	elementary-data事例：API「secretsmanager:GetSecretValue」を用いて平文状態の認証情報を取得
遠隔操作 （Command and Control）	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）	T1071.001	両事例：HTTPSプロトコルを用いて攻撃者のC&Cエンドポイント宛に情報流出
遠隔操作 （Command and Control）	デッドドロップ・リゾルバ （Dead Drop Resolver）	T1102.001	KICSおよびBitwardenの亜種は、GitHubのコミット検索APIを用いてフォールバック復旧用のC&Cドメインを取得
情報流出 （Exfiltration）	C&Cチャネルを介した情報流出 （Exfiltration Over C2 Channel）	T1041	両事例：認証情報のアーカイブを暗号化し、HTTPSを通して主要なC&Cエンドポイントに送信
情報流出 （Exfiltration）	Webサービスを通した情報流出 （Exfiltration Over Web Service）	T1567	KICS事例：小説「Dune」を思わせる名前のGitHub公開リポジトリを自動作成し、デッドドロップの置き場として利用
Impact （影響）	金銭の奪取 （Financial Theft）	T1657	elementary-data事例：暗号資産ウォレット情報を収集