サイバー攻撃知識ベース「MITRE ATT&CK」との紐づけ

Tactics （戦略）	Techniques （技術）	関連箇所
Reconnaissance （偵察）	T1595.002 Active Scanning: Vulnerability Scanning （アクティブスキャン：脆弱性スキャン）	10個のユーザエージェントを使い分け、5秒の間に「/health」や「/api/v1/version」、「/manifest.json」などに対するスキャン活動を実行；別のスキャナーからユーザエージェントを流用し、RCE脆弱性（CVE-2025-3248）を探索
Resource Development （リソース開発）	T1588.002 Obtain Capabilities: Tool （機能獲得：ツール）	独自のXMRigマイナー（ procq ）をC&Cサーバから 圧縮アーカイブ「ks.tar」 としてダウンロード；中身はコンパイル済みであり、28種のハッシュ化アルゴリズムに対応する他、ユーザエージェントの偽装機能も搭載
Initial Access （初期アクセス）	T1190 Exploit Public-Facing Application （公開アプリケーションの悪用）	URL「/api/v1/build_public_tmp/{フローID}/flow」に不正なPOSTリクエストを送信；脆弱性「CVE-2026-33017」を悪用したもので、未認証のままPythonコードを実行
Execution （実行）	T1059.004 Command and Scripting Interpreter: Unix Shell （コマンド/スクリプトのインタプリタ：Unixシェル）	「curl l sh」のコマンド形式によるドロッパチェーン；「isp.sh」を通した水平移動・内部活動
	T1059.006 Command and Scripting Interpreter: Python （コマンド/スクリプトのインタプリタ：Python）	Langflowの「CustomComponent.value」において、eval 関数を悪用；攻撃者が送り込んだペイロードが、アプリ自体のプロセスにより、Pythonコードとして稼働
	T1106 Native API （ネイティブAPI）	Go言語の標準API「os/exec.Command」を通してシェルコマンド（runCmd、startMiner、crontab）を実行
Persistence （永続化）	T1053.003 Scheduled Task/Job: Cron （タスク/ジョブのスケジュール起動：Cron）	crontabに727バイトの設定内容を登録
	T1543.004 Create or Modify System Process: Systemd （システムプロセスの作成や改変：Systemd）	「/etc/rcS.d」を悪用し、システム起動時にセキュリティ機能「AppArmor」を無効化
Defense Evasion （防御回避）	T1027 Obfuscated Files or Information （ファイルやデータの難読化）	マイナーの実行ファイルを、「ドット」と「スペース」を組み合わせた3層ネストのディレクトリ「./. /. /procq」に隠蔽；プロセス名を「procq」にすることで、システムプロセスに偽装
	T1036.005 Masquerading: Match Legitimate Name or Location （なりすまし：正規の名前や場所）	マイナー「procq」は、マイニングプールにJSON-RPC形式でログインする際、ユーザエージェントを「SystemMonitor/6.25.0」に設定することで、システム監視ツールとして偽装
	T1070.002 Indicator Removal: Clear Linux Logs （痕跡の消去：Linuxログの消去）	コマンド「rm -rf /var/log/syslog」を実行
	T1070.004 Indicator Removal: File Deletion （痕跡の消去：ファイルの削除）	コマンド「rm -rf /var/log/syslog」を実行；今回確認された唯一のログ削除コマンド
	T1140 Deobfuscate/Decode Files or Information （ファイルやデータの難読化解除またはデコード）	UPXで難読化されたlambsys のバイナリを利用；関数「unarchiveTarGz()」を利用してアーカイブ「ks.tar.gz」を展開；ダウンロードしたペイロードのMD5ハッシュ値を検証
	T1222 File Permissions Modification （ファイル権限の変更）	競合相手によるロックを解除するため、コマンド「chattr -iua」を「cron」や「/tmp」、「/var/tmp」、SSH関連パス（「~/.ssh/」、「~/.ssh/authorized_keys」）に一斉適用；自身のペイロードを保護するため、コマンド「chattr +iua」を「/var/tmp」や「/tmp」に適用
	T1489 Service Stop （サービス停止）	以下のコマンドによってセキュリティサービスを停止 service apparmor stop; systemctl disable apparmor; service aliyun.service stop; systemctl disable aliyun.service; systemctl stop c3pool_miner.service
	T1562.001 Impair Defenses: Disable Tools （防御機能の阻害：ツールの無効化）	AppArmor、SELinux、NMI watchdog、Aliyunのクラウドセキュリティエージェントを無効化
	T1562.004 Impair Defenses: Disable Firewall （防御機能の阻害：ファイアウォールの無効化）	コマンド「ufw disable」や「iptables -F」を実行
	T1564.001 Hide Artifacts: Hidden Files and Directories （アーティファクトの隠蔽；ファイルやディレクトリの隠蔽）	ドットとスペースだけの特殊なパス「./. /. /procq」にマイナーのバイナリを隠蔽；プロセスIDの管理用ファイルを、「/tmp/.X11-unix/」や「/tmp/.systemd.*」といったOSシステムを思わせる場所に配備
	T1574.006 Hijack Execution Flow: Dynamic Linker Hijacking （実行フローの乗っ取り：動的リンカーの乗っ取り）	ファイル「/etc/ld.so.preload」の保護属性を解除（chattr -i）した上で完全削除（ rm -f ）；監視ツールなどによるLD_PRELOADフックを阻止
Credential Access （認証情報アクセス）	T1552.004 Unsecured Credentials: Private Keys （安全でない認証情報：秘密鍵）	スクリプト「isp.sh」の関数「b()」により、「id_rsa/id_ed25519/id_dsa」の内容や、ssh-agentが読み込んでいる鍵データを入手；水平移動・内部活動に利用
Discovery （探索）	T1016 System Network Configuration Discovery （システムネットワーク設定の探索）	接続可能なホストをさぐるために「known_hosts」の中身を解析；ネットワークインターフェースの詳細情報を取得
	T1057 Process Discovery （プロセスの探索）	ライバルのマイナーを検知
	T1082 System Information Discovery （システム情報の探索）	「/etc/os-release」の読み込み；DMIの調査； コマンド「uname」
	T1083 File and Directory Discovery （ファイルやディレクトリの探索）	本処理に入る前に、自身のマイナー本体「procq」が存在しているか確認；「/tmp」をスキャンし、ライバルのPIDファイルを探索
	T1614 System Location Discovery （システム位置情報の取得）	乗っ取ったサーバの位置情報を把握するため、「ipinfo[.]io」を通してDNSルックアップを実施（ANY.RUN run-2 Suricata SID 2054168）
Lateral Movement （水平移動・内部活動）	T1021.004 Remote Services: SSH （リモートサービス：SSH）	「known_hosts」と「ssh-agent」を利用し、SSHワームの機能を実行

Command and Control （遠隔操作）	T1071.001 Application Layer Protocol: Web Protocols （アプリケーション層プロトコル：Webプロトコル）	「/status.php」宛てにHTTP POSTリクエストを送信
	T1105 Ingress Tool Transfer （外部からのツール取得）	curl や wgetを用いてC&Cサーバからlambsysのバイナリをダウンロード； ダウンロードしたアーカイブ「ks.tar」のMD5ハッシュ値を検証；再ダウンロードによる自己修復のループ機構
	T1132.001 Data Encoding: Standard Encoding （データエンコード：標準エンコード方式）	C&Cサーバへのステータス連絡には、標準的なJSONシリアライズ形式を使用 {"downloading":false,"running":true,"timestamp":...}
Exfiltration （情報流出）	T1020 Automated Exfiltration （情報流出の自動化）	C&Cサーバの「/status.php」に対して定期的にステータス情報を自動発信；古い亜種は「/r.php」に対して被害者IPを送信
Impact （影響）	T1496 Resource Hijacking （リソースの乗っ取り）	独自仕様のXMRigマイナー「procq」は「RandomX」の仕組みを搭載；マイナーのウォレット情報（47VVuaLN...JkjbZT31）；偽装ユーザエージェント「SystemMonitor/6.25.0」；28種のハッシュ化アルゴリズムに対応；2024年版も2026年版も同じks.tarをダウンロード（MD5も一致）；サンドボックス環境での稼働はなし
	T1531 Account Access Removal （アカウントアクセスの削除）	ライバルのグループが作成したアカウント「akay」と「vfinder」を削除