

戦術 (Tactic)	技術 (Technique)	ID	説明
初期侵入	リムーバブルメディアを介した複製	T1091	HIUPAN はリムーバブルドライブを介して拡散し、PUBLOAD を配信する
	フィッシング：スパイ フィッシング添付ファイル	T1566.001	スパイフィッシングメールを使用して標的のシステムにアクセスを獲得する
永続化	起動時または自動実行： レジストリ実行キー/ スタートアップフォルダ	T1547.00	永続化のためにレジストリ実行キーを使用する
	スケジュールされたタスク/ ジョブ：スケジュールされたタスク	T1053.005	永続化のためにスケジュールされたタスクを使用する
検出回避	実行フローのハイジャック： DLL サイドローディング	T1574.002	複数のマルウェアが DLL サイドローディングを使用して読み込まれる
	実行ガードレール：環境 キーイング	T1480.001	第2段階の PLUGX ペイロードは RC4 と DPAPI で保護されている
	信頼制御の回避：コード 署名	T1553.002	DOWNBAIT はデジタル署名されている
	プロセスインジェクション	T1055	PLUGX は様々な引数で起動された他のプロセスにコードを注入する
事前調査	システム情報の探索	T1082	hostname や systeminfo などのコマンドを使用してシステム情報の探索を行う
	ソフトウェアの探索：セキュリティソフトウェアの探索	T1518.001	Wmic を使用してインストールされた AV 製品を探索する
	システムネットワーク接続の探索	T1049	Netstat を使用してネットワーク接続を探索する
	システムネットワーク設定の探索	T1016	ipconfig や netsh などのコマンドを使用してネットワーク設定を探索する

情報収集	ローカルシステムからのデータ	T1005	FILESACを使用してシステム内の特定のファイルタイプを検索する
	収集データのアーカイブ：ユーティリティによるアーカイブ	T1560.001	WinRARまたはFILESACを使用して収集したデータをアーカイブする
情報送付	Webサービスを介した流出：クラウドストレージへの流出	T1567.002	テレメトリ情報がクラウドサービスへの可能な流出を示唆している
	代替プロトコルを介した流出	T1048	データは攻撃者が管理するサーバーにcURLまたはPTSOCKETを使用して流出させる
コマンド&コントロール	アプリケーション層プロトコル：Webプロトコル	T1071.001	ダウンローダーやバックドアはHTTP/HTTPSを使用してC&Cと通信する