コマンドID	概要
0x10	対話型シェル（PTY）を生成し、入出力（Input / Output）をC&Cサーバにバインドする
0x20	/proc/mountsを構文解析（パース）し、マウント（認識）されたファイルシステムを列挙する
0x22	ディレクトリ内のファイルを列挙し、ファイル名、サイズ、タイムスタンプを返す
0x24	unlinkを用いてファイルを削除する、または、/bin/rm -rfを用いてファイルを再帰的に削除する
0x25	rename関数を用いてファイル名変更または移動を行う
0x26	mkdirを用いて新たなディレクトリを作成する
0x27	最大10MBのファイルをメモリ内に読み込み、C&Cサーバに送信する
0x29	指定されたファイルパスに特定のテキストデータを書き込む
0x30	64KB単位のファイルチャンクを読み取り、C&Cサーバに送信する
0x31	C&Cサーバから受信したファイルチャンクをディスクに書き込む
0x33	アクティブなファイルアップロードタスクまたはダウンロードタスクを中止する
0x40	CPU、RAM、GPU、ディスク使用率、ネットワークインターフェイスの統計情報などを窃取する
0x42	/proc/[pid]/commを読み取り、稼働中のプロセスを列挙する
0x44	curl/wgetを用いてペイロードをダウンロードする、または、execvpを用いてローカル環境のバイナリを実行する
0x45	kill(pid, 9)を用いて指定されたプロセスを強制終了する
0x50	/proc/net/tcpを構文解析し、アクティブなネットワーク接続を一覧表示する
0x52	ss --killを用いて特定のTCP接続を切断する
0x60	shutdownまたはsystemctlを用いて感染システムの再起動、一時停止、中止を実行する
0x61	セッションリセットフラグを設定し、C&Cサーバへの再接続を強制する
0x62	現在のソケット接続を切断し、再接続と同じ処理を行う
0x63	自己削除機能を起動し、永続化手法やバイナリを削除する
0x64	sudoまたはpkexecを用いてQLNXをroot権限で再実行しようと試みる
0x65	curl/wgetを用いてバッククラウンドでURLを開く、または、xdg-openを用いて表示する
0x66	notify-sendを用いてデスクトップ通知を表示する
0x70	QLNXのエントリを確認するためにsystemd、crontab、init.d、bashrc、ld.so.preloadをスキャンする
0x72	指定された永続化手法を用いてマルウェアをインストールする
0x73	指定された永続化手法からマルウェアを削除する
0x80	生のTCPソケットを開き、標的ホストやポートへのプロキシ接続を確立する
0x82	確立されたTCPトンネル経由で生データを送信する
0x83	アクティブなTCPトンネルを閉鎖する
0x90	SSH鍵、ブラウザデータベース、クラウドトークン、クリップボードデータを抽出する
0xA0	特定のIPアドレス範囲に対してマルチスレッドTCPポートスキャンを実行する
0xA2	スクリーンショットを撮影して、C&Cサーバに送信する
0xB0	/dev/inputまたはX11環境を用いてキー入力操作情報の窃取を開始する
0xB1	アクティブなキー入力操作情報窃取スレッドを停止する
0xB3	ptraceまたは/proc/pid/memを用いて特定のプロセスにシェルコードを注入する
0xB5	共有ライブラリをメモリから直接読み込む
0xB7	窃取したSSH認証情報を用いてリモートホスト上でコマンドを実行する
0xB9	SSHの設定ファイルおよび鍵情報を構文解析し、内部活動の対象を特定する
0xBB	PAM認証処理悪用モジュールを用いて、認証情報を窃取する
0xBD	/etc/ld.so.preloadを用いてユーザ空間にルートキットをインストールする
0xC0	脆弱性悪用手口（エクスプロイト）やモジュールの実効性を検証する
0xD0	メモリ上でBeacon Object File（BOF）を実行する
0xD4	ローカルポートをバインドし、トラフィックをリモート先へ転送する
0xD6	アクティブなポート転送ルールを用いてデータを送信する
0xD7	アクティブなポート転送ルールを終了する
0xD8	感染ホスト上でSOCKSプロキシサーバを起動する
0xD9	アクティブなSOCKSプロキシサーバを停止する
0xDC	クリップボードや画面の継続監視を開始する
0xDD	継続監視を終了する
0xE0	プロセスID、ファイル、ネットワークポートを隠蔽するためeBPFマップを読み込む
0xE4	P2Pルーティングテーブルを管理する
0xE6	ファイルブラウザデータをP2Pメッシュネットワーク経由で送信する
0xE8	システムログ（auth.log、syslog、wtmp、bash_history）を消去する
0xEA	PAM認証フックをインストールまたは削除する
0xEE	notifyを用いて指定されたパスに対するリアルタイムファイルシステム監視を設定する（作成、削除、変更、移動）
0xEF	アクティブなinotify監視をすべて削除する
0xF2	utimensatを用いてファイルのタイムスタンプを改ざんする