

ファイル名	内容
cmd.aspx cmd2.aspx default.aspx	<ul style="list-style-type: none"> クライアントから受信したフォーム「Request.Form["command"]」の内容に基づき、任意のコマンドシェルコードを実行する。 コマンドの実行結果をクライアントに返却する。
0514_Bills_Payment_Intraday_01102019_114424.aspx	cmd.aspx に類似するが、任意のコマンドを実行する手段として、cmd.exe の代わりに powershell.exe を使用する。
514_Bills_Payment_Intraday_01012019_054034.aspx	<ul style="list-style-type: none"> 任意のファイル管理、操作を実行できる可能性がある。 ファイルやフォルダのナビゲーション、作成、編集、削除を行う。 アップロード機能があり、コンポーネントの拡充に使用される可能性がある。
cmd.asp	<ul style="list-style-type: none"> URL「?cmd={コマンド}」を添えてアクセスすることで、任意のコマンドラインを実行できる。実行結果は、アクセス元に返される。 該当する URL 例："www[.]example.com/cmd.asp?cmd={コマンド}"
hello.aspx	「hello」という文字列のみが記載されている。
up.aspx up.html	<ul style="list-style-type: none"> 任意のファイルをアップロードする機能を持つと見られる。サーバ内で発見された他の不正なスクリプトも、本機能によってアップロードされた可能性がある。 メソッド「FileUploadControl.SaveAs()」：サーバ側にアップロードされたファイルを、内容のサニタイジングや形式のバリデーションなしで、そのまま保存する。 FileUploadControl.FileName：重要なサーバファイルの削除や、ディレクトリトラバーサルに利用される。サニタイジングはスキップする。
0x02.exe	<ul style="list-style-type: none"> 検体を展開したところ、ランタイムのデバッグログとして、フィリピン語と英語の双方が使用されていることが分かった。これは、比較的珍しいパターンである。ランタイムのデバッグ文字列にローカル言語が使用されていることは、実際に攻撃者が当該言語の話者であることを示唆する一方、そのように思い込ませ、自身が特定されないように画策している可能性もある。 名前付きパイプやリモートプロシージャプロトコル（RPC：Remote Procedure Protocol）を経由して任意のコマンドを実行する。 本機能を利用する上では、先述の VC ランタイム DLL を用意した上で、適切な引数を指定する必要がある。 <ul style="list-style-type: none"> -c：名前付きパイプや RPC 経由で実行するコマンド -d：セッション ID -i：権限継承のオプション -h：ヘルプ用のオプション 「なりすまし」や「セキュリティ定義の変更」など、さまざまな手段によって権限昇格を行う。 RPC 機能や名前付きパイプの作成、接続を行う。 パイプの応答データに含まれるコマンド引数をもとに、プロセスを作成する。