タイムスタンプ	観察	影響を受ける資産
6/23/25 10:07:11.000 AM	WebShell（ws.phtml）を通じて `whoami` コマンドを実行を確認。 uploads → ファイルアップロード機能経由で置かれた可能性が高い。 ここでws.phtmlが最初にアクセスしたファイルと判断。	WEB01
6/23/25 11:44:19.354 AM	Web サーバ侵害後に、権限昇格調査ツール（linPEAS）を外部からダウンロードしている	WEB01
6/23/25 11:44:34.013 AM	linpeas.sh に実行権限を付与しているのを確認。	WEB01
6/24/25 6:37:52.000 AM	外部HTTP サーバからSharPersist.exe をダウンロードし、net.exeとして保存	DC01
6/24/25 6:45:59:000 AM	外部HTTP サーバからbits.exe をダウンロードし、bits.exeとして保存	DC01
6/24/25 6:45:59:000 AM	tasksにbits.exeが置かれているのを確認	DC01
6/24/25 6:50:16.000 AM	新規にbitssを登録されているのを確認	DC01
6/24/25 12:41:51.000 PM	horilla.zipをPowerShell の Compress-Archiveコマンドで、 特定のフォルダを ZIP に圧縮して別の場所に保存	HRIS
6/24/25 12:45:45.000 PM	horilla.zip の持ち出しを確認	HRIS
[...]	[...]	[...]