# Investigation(Aside): OilRig Case Study

## Webshells used by OilRig and their respective goals

| Webshell | Goal |
|---|---|
| **HyperShell** | • Variant of the TwoFace loader which when decrypted, **drops the webshell, HighShell**. |
| **HighShell v5.0** | • Variant of the TwoFace payload with two exceptions in the user interface, a **version number** and a means of displaying **error messages and command results**.<br>• Also includes a **salt value** applied to the actor-provided password for authentication.<br>• Another variant of HighShell v5.0 introduced an **explorer tab** to navigate the file system of the compromised server. |
| **HighShell v7.1** | • Expanded to **split main functionality** across multiple tabs, 'Command', 'Explorer', 'Upload', 'SQL Server' and 'Change Time'. |
| **HighShell v8.6.2/v8.8.5** | • **Enhanced user interface**.<br>• Includes a **front end** user interface that interacts with a back end script via AJAX web requests.<br>• **New executable modules** '**7za**' to archive files from the Explorer tab, '**nbtscan**' to scan the network for systems to build an IP list it can interact with and '**rx**' for remote execution.<br>• The **Network downloader** functionality to allow the actor to quickly upload user files from remote victim systems and rapidly check for the creation of new files by network users.<br>• The **spy check** feature that compares the SHA256 hash of the HighShell front end to notify the actor to avoid using the webshell in the event of modification of the webshell. |
| **Minion** | • Variant of HighShell.<br>• **Extends functionality** by including modules '**Hobocopy**', a backup/copy tool and '**Tardigrande**' a port-scanning, screenshot tool. |

## Logical abstraction to get to writing indicators of compromise

| IOC | Tool Used | Data required to analyse | Logical abstraction to get to IOC |
|---|---|---|---|
| **Poison Frog / Myleftheart[.]com** | Poison Frog (backdoor) | The dropper '**poisonfrog.ps1**' which installs the poison frog agents '**hUpdater.ps1**' that uses HTTP for C2 and '**dUpdater.ps1**' that uses DNS tunneling for C2. | ● For the agent, there should be a server that would allow the actor to interact with the compromised system.<br>● Both of the poison frog agent scripts were configured to use this domain as its C2 server. |
| **office365-management[.]com (185.162.235[.]29)**<br><br>**msoffice-cdn[.]com (185.162.235[.]121)** | DNS Hijacking Script | An example adversary IP for the legitimate domain to be redirected to. | ● The examination of the Class C IP block of 185.162.235[.]0/24 showed these domains which were previously identified as C2 servers for OilRig. |
| **185.162.235[.]106** | DNS Hijacking Script | Analysis of the IP. | ● The analysis of this IP provided possible relationships to previous OilRig infrastructure.<br>● The examination of the hosting provider showed that this IP was associated with an Iranian hosting provider called NovinVPS.<br>● The autonomous system name of the IP showed that the allocation was controlled by Serverius Holding B.V., which was previously associated with OilRig. |
| **185.161.209[.]57 / 185.161.210[.]25** | Administrative panel for a VPS account on DeltaHost | Screenshots of web browser sessions into VPS administrative panels. | ● These IPs were listed in the panel and were in the same range as an IP associated with the DNSpionage campaign. |

| | | | |
|---|---|---|---|
| | | | • The combination of the use of DeltaHost and IPs belonging to a fairly small range. |
| **OopsIE payload / 193.111.152[.]13** | Administrative panel for a VPS account on DeltaHost | Screenshots of web browser sessions into VPS administrative panels. | • Observation of an organisation targetted by OilRig downloading a zip archive '[redacted]-ITsoftwareUpdate.exe', a variant of the OopsIE Trojan from this address, suggesting the server was in use by OilRig at the time. |
| **164.132.67[.]216** | Glimpse (backdoor) | Screenshots of remote desktop (RDP) sessions showing the Glimpse panel. | • Screenshot in leak of RDP session with a server running the Glimpse C2. |
| **142.234.157[.]21** | Scarecrow (backdoor) | Screenshots of web browser sessions displaying the Scarecrow panel. | • The server of this backdoor is hosted on this address and it is evident in the snapshot that multiple systems were compromised. |