BRAVO FIVE

MISSION BRIEF

Black Bag Challenge

BSides 2023

SITUATION

General

After being denied membership of NATO due to outstanding questions arising from known clandestine operations in the Second Congo War, the small nation of Burligrifistan is openly supporting Russia in the invasion of Ukraine.

Initially support was provided as materiel and political influence. Since the latest round of sanctions against Russia, Burligrifistan has pivoted to providing full support of international operations outside of the main Ukrainian theatre in order to influence or degrade assistance provided to Ukraine by its allies, with strong intent to target Five Eyes nations.

Enemy

Burligrifistan (https://burligrifistan.xyz) is a small nation bordering Russia, Georgia, Azerbaijan, and the Caspian Sea. Historically a city state vassal to the Persian Empire across the Caspian Sea, it was used as a shipping gateway to other ports. After World War II Burligrifistan was part of the Soviet Union. Moscow, seeing the potential in the land and largely unencumbered infrastructure of Burligrifistan poured migrants from overcrowded or irradiated (post-Chernobyl) eastern European cities into the country, effectively overwhelming the ancient Persian cultural influences. Now Burligrifistan resembles an out of place Eastern European state straddling the Asian and European continents.

The Burligrifistan Armed Defence (BAD) is the state military. The BAD is known for strong espionage and clandestine operations capabilities, however are technologically deficit in most areas other nations consider commonplace. The most striking example of this is the lack of Burligrifistanian cyber capability. The state does not operate strategic-level offensive or defensive cyber capabilities, and it is largely left to the individual force elements of the BAD to provide cyber effects and security on operations.

The special operations arm of the BAD is the Burligrifistan Special Operations Department (BSOD). They are known for taking direct action as a first option to solving almost any scenario. This has left the state few friends in the international community. Their common tactics, techniques, and procedures include: sabotage, espionage, counter-intelligence, assassinations, kidnappings, and supply chain interdiction.

Intelligence reports indicate that a BSOD operative is operating in the area and staying at the Charnwood Manor motel. Their identity and intentions are unknown.

Friendly

The Direct Espionage Service (DES) has the remit to disrupt and exploit BSOD operatives in the local area. As part of a local counter-espionage operation three independent task units have been deployed into this area of operations. Each task unit contains two teams. The units are Alpha Four, Bravo Five, and Charlie Six. Alpha is awaiting tasking, and ready, and Charlie is the designated quick reaction force.

While on mission Bravo is able to request QRF from Charlie, at five minutes notice to move and 15 minutes time-to-station.

Area

The mission area is centred on the Charnwood Manor motel, in Charnwood ACT.

MISSION

Bravo Five is to exploit all relevant systems and media within room 88 of the Charnwood Manor and remain undetected IOT maximise intelligence gain/loss on the BSOD operative and BSOD operations.

EXECUTION

It is imperative that no elements of Bravo Five are detected during this operation. No intelligence is worth the potential diplomatic incident that may result. In all situations, relinquish before compromise.

Troops to task

Bravo Five team one of the DES (B51DES) is tasked as the exploitation team. You are to:

- Gain access to room 88
- Exploit all systems in the room
- Exploit all media, digital or paper in the room
- Place a listening device within the room where it is unlikely to be detected
- Execute and persist an software implant on any of the target's devices
- Retain all intelligence gained from exploitation activities
- Remain in contact with Bravo Five Two
- Leave no indication that the room has been exploited
- Leave no indication that systems or physical security measures have been accessed

Bravo Five team two of the DES (B52DES) is tasked as the target surveillance team. You will surveil the target during the time window B51 has access to the room and:

- Observe target activities and report on any pertinent movements.
- Intercept target conversations and report on any pertinent information to Bravo Five One.
- Remain undetected.

Likely exploitation activities

The target is likely in possession of the following media types which may require exploitation to extract intelligence:

- Laptop with spinning or solid state drive.
- Removable media, such as a USB stick or external solid state hard drive.
- Paper, including whole dossiers or single sheets.
- Inbuilt digital storage in optical or audio devices such as cameras or other IoT devices.

Additionally media may have physical or digital protections such as:

- Locked physical container for paper or digital media.
- Encryption applied to digital media.
- Media may be hidden in the room in an effort to obscure it from staff or adversaries.
- Media or devices may use biometrics.

Implant

You will be supplied with an executable implant file on removable media. After gaining access to the target's device/devices B51 is to:

- Execute a covert implant as a privileged user or system.
- Persist the implant so it remains in place through reboots and attempts to remove it.
- Obfuscate the implant so it is not easily discovered.

After execution the implant will confirm effective persistence and obfuscation.

It is unlikely the targets machine has effective active defences (such as application control, anti-virus, or host intrusion detection), however they are known to manually run custom scanning programs regularly.

You may bring and use whatever software you require to achieve the implant tasks.

Admin & Logistics

Once in the staging area B51 will have access to following tools and materials for their mission. Use is optional, you can take or leave whatever you wish.

- HDD dock
- Lockpicks
- Screwdriver set
- Endoscope
- Duty bag
- Deployable video camera and screen
- Fingerprint kit
- Portable battery powered printer
- Hi-vis vests
- Torches
- UV torches
- Doorstop

All items must be signed out prior to the mission. Teams may also bring whatever they wish into the room, provided the tool or item is not destructive to the room, or electronic devices. Operational security must be maintained.

Reports

Reports of intelligence collected is due 120 minutes after mission debrief. Intelligence collected can be reported to the secure team flag submission server at https://blackflag.redacted.au. Your password will be sent to you.

Command & Signals

Timings

Your mission timeframe has already been confirmed. Teams are to arrive at the staging area **10 minutes** before the mission start. Arriving late will consume available mission time.

The staging area is outside the Black Bag (The DERWENT Room).

From intelligence we know that the target has a meeting in the hotel bar which is scheduled to run for about 15 minutes. This is likely the time Bravo Five One will have to execute their tasks.

Command

Operational commanders can be identified wearing the Direct Espionage Service motto on their front: “How good is your OPSEC?”. All direction by these personnel is to be followed.

Bravo Five Two has command of the mission start. Their team will confirm, over radio, when the target has moved to the hotel bar and it is safe for Bravo Five One to commence.

BRAVO FIVE ONE is NOT to commence until they have radio confirmation that the target is out of the mission area.