```
import "pe"

rule APT_RU_BlueDelta_Headlace {

    meta:
        description = "Detects BlueDelta's Headlace BAT script"
        version = "1.0"
        hash = "19e95b32b77d8dfd294c085793cd542d82eddac8e772818fea2826fa02a5cc54"
        hash = "e373a2e8288608757c4716910270747f38184c68114f09ee08e155f1b094a120"
        hash = "f5b7a2d9872312e000acbe3dc8153707acecc5ba184f97ad6014327db16549c7"
        RF_THREATACTOR = "BlueDelta"
        RF_MALWARE = "Headlace"
        RF_MALWARE_ID = "txvlKg"
        RF_THREATACTOR_ID = "L37nw-"

    strings:
        $ = "chcp 65001"
        $ = "taskkill /im msedge.exe"
        $ = "msedge --headless=new --disable-gpu "
        $ = "%userprofile%\\Downloads\\*.css"
        $ = "del /q /f"

    condition:
        filesize < 15KB and
        all of them
}

rule APT_RU_BlueDelta_Headlace_DLL
{
    meta:
        description = "Detects a sideloaded DLL used to execute Headlace"
        version = "1.0"
        hash = "9a798e0b14004e01c5f336aeb471816c11a62af851b1a0f36284078b8cf09847"
        hash = "c968f9dd1f16a435901d2b93a028a0ae2508e943c8f480935a529826deb3dbeb"
        RF_MALWARE = "Headlace"
        RF_MALWARE_ID = "txvlKg"
        RF_THREATACTOR = "BlueDelta"
        RF_THREATACTOR_ID = "L37nw-"

    strings:
        /*
            0x180001000 4883EC28                    sub rsp, 28h
            0x180001004 83FA01                      cmp edx, 1
            0x180001007 750D                        jne 180001016h
            0x180001009 488D0D90110000              lea rcx, [rip + 1190h]
            0x180001010 FF15CA100000                call qword ptr [rip + 10cah]
            0x180001016 B801000000                  mov eax, 1
            0x18000101b 4883C428                    add rsp, 28h
            0x18000101f C3                          ret
        */
```

```
        $c1 = {
            48 83 EC 28
            83 FA 01
            75 ??
            48 8D 0D ?? ?? ?? ??
            FF 15 ?? ?? ?? ??
            B8 01 00 00 00
            48 83 C4 28
            C3
        }

        /*
            0x180001000 4883EC28                    sub rsp, 28h
            0x180001004 83FA01                      cmp edx, 1
            0x180001007 740A                        je 180001013h
            0x180001009 B801000000                  mov eax, 1
            0x18000100e 4883C428                    add rsp, 28h
            0x180001012 C3                          ret
            0x180001013 488D0D86110000              lea rcx, [rip + 1186h]
            0x18000101a FF15C0100000                call qword ptr [rip + 10c0h]
            0x180001020 33C0                        xor eax, eax
            0x180001022 4883C428                    add rsp, 28h
            0x180001026 C3                          ret
        */

        $c2 = {
            48 83 EC 28
            83 FA 01
            74 ??
            B8 01 00 00 00
            48 83 C4 28
            C3
            48 8D 0D ?? ?? ?? ??
            FF 15 ?? ?? ?? ??
            33 C0
            48 83 C4 28
            C3
        }

    condition:
        pe.is_dll() and
        (
            pe.pdb_path contains "PROJECTS\\Dll1" or
            pe.number_of_exports == 0
        )
        and 1 of them
}
```