

Possible Pakistan-nexus Backdoor Targeting Afghanistan

 dmpdump.github.io/posts/Backdoor_Targeting_Afghanistan

September 15, 2026

On August 29, 2026, a ZIP file containing an executable named Special Job Opportunities and Recruitment Information in Various Ministries of Afghanistan.exe and a DLL named dxgi.dll was uploaded to Virus Total from Afghanistan. The executable name and the upload origin suggest the likely targeting of an Afghanistan government agency. As expected, the executable is a legitimate executable (ApplicationFrameHost.exe, a Windows executable), and the DLL is a malicious library that is side-loaded by the renamed executable.

Name	Type	Size
 dxgi.dll	Application extension	457 KB
 Special Job Opportunities and Recruitment Information in Various Ministries of Afghanistan.exe	Application	79 KB

Figure 1: Zip content.

A review of the side-loaded DLL revealed a targeted backdoor using the following C2:
185.235.137[.]35:9000.

Backdoor Overview

The DLL establishes persistence by making a copy of the renamed ApplicationFrameHost.exe executable using GetModuleFileNameW to retrieve its own path and copying itself and the accompanying DLL to %AppData%\Microsoft\ApplicationHost\. The executable is copied as ApplicationHost.exe. Persistent execution is established using the common registry run key HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

```

if ( SHGetFolderPathW(0LL, 26, 0LL, 0, pszPath) )
    return 0;
memset(v16, 0, sizeof(v16));
v1 = -1LL;
do
    ++v1;
while ( pszPath[v1] );
sub_180008DC0(v16, (__int64)pszPath, v1);
v2 = sub_180008F20(v16, L"\\Microsoft\\ApplicationHost\\ApplicationHost.exe", 46LL);
v3 = *(_OWORD *)v2;
v17[0] = *(_OWORD *)v2;
v4 = *(_m128i *)(v2 + 16);
v17[1] = v4;
*(_QWORD *)(v2 + 16) = 0LL;
*(_QWORD *)(v2 + 24) = 7LL;
*(_WORD *)v2 = 0;
sub_180008EA0(v16);
if ( RegOpenKeyExW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", 0, 2u, &phkResult) )
{
    v5 = 0;
}

```

Figure 2: Registry run key.

The main backdoor logic is implemented in an exported function named `DXGIDeclareAdapterRemovalSupport()`. First, this function implements anti-debugging and anti-analysis checks:

- It detects debuggers with `CheckRemoteDebuggerPresent()` and `OutputDebugStringA()` timing.
- It detects the presence of common analysis tools: `ida.exe`, `ida64.exe`, `x64dbg.exe`, `x32dbg.exe`, `windbg.exe`, `ollydbg.exe`
- It performs timing and integrity checks.

```

bool fn_antidebug()
{
    HANDLE CurrentProcess; // rax
    DWORD TickCount; // ebx
    BOOL pbDebuggerPresent; // [rsp+20h] [rbp-18h] BYREF

    pbDebuggerPresent = 0;
    CurrentProcess = GetCurrentProcess();
    CheckRemoteDebuggerPresent(CurrentProcess, &pbDebuggerPresent);
    if ( pbDebuggerPresent )
        return 1;
    TickCount = GetTickCount();
    OutputDebugStringA("AntiDebugCheck");
    return GetTickCount() - TickCount > 100;
}

```

Figure 3: Sample anti-debugging.

```

char fn_anti_analysis_tool_check()
{
    HANDLE Toolhelp32Snapshot; // rax
    void *v1; // rsi
    unsigned int v3; // ebx
    const __m128i **v4; // rdi
    _QWORD v5[6]; // [rsp+40h] [rbp-288h] BYREF
    PROCESSENTRY32 pe; // [rsp+70h] [rbp-258h] BYREF
    __m128i MultiByteStr[17]; // [rsp+1A0h] [rbp-128h] BYREF

    v5[0] = "ida.exe";
    v5[1] = "ida64.exe";
    v5[2] = "x64dbg.exe";
    v5[3] = "x32dbg.exe";
    v5[4] = "windbg.exe";
    v5[5] = "ollydbg.exe";
    Toolhelp32Snapshot = CreateToolhelp32Snapshot(2u, 0);
    v1 = Toolhelp32Snapshot;
    if ( Toolhelp32Snapshot == (HANDLE)-1LL )
        return 0;
    pe.dwSize = 304;
    if ( Process32First(Toolhelp32Snapshot, &pe) )
    {
        while ( 2 )
        {
            WideCharToMultiByte(0, 0, (LPCWCH)pe.szExeFile, -1, MultiByteStr[0].m128i_i8, 260, 0LL, 0LL);
            sub_1800200F0(MultiByteStr, 260LL);
            v3 = 0;
            v4 = (const __m128i **)v5;
            do
            {
                if ( sub_18001B084(MultiByteStr, *v4) )
                {
                    CloseHandle(v1);
                    return 1;
                }
                ++v3;
                ++v4;
            }
            while ( v3 < 6 );
            if ( Process32Next(v1, &pe) )
                continue;
            break;
        }
    }
}

```

Figure 4: Sample anti-analysis.

The backdoor checks if it is being executed with the `--startup` argument. If it is not, it drops and opens an embedded decoy PDF named `Document_<4digits>.pdf` under `AppData\Roaming\`. The `--startup` argument is likely used by the malware developer to avoid dropping the PDF with each test run.

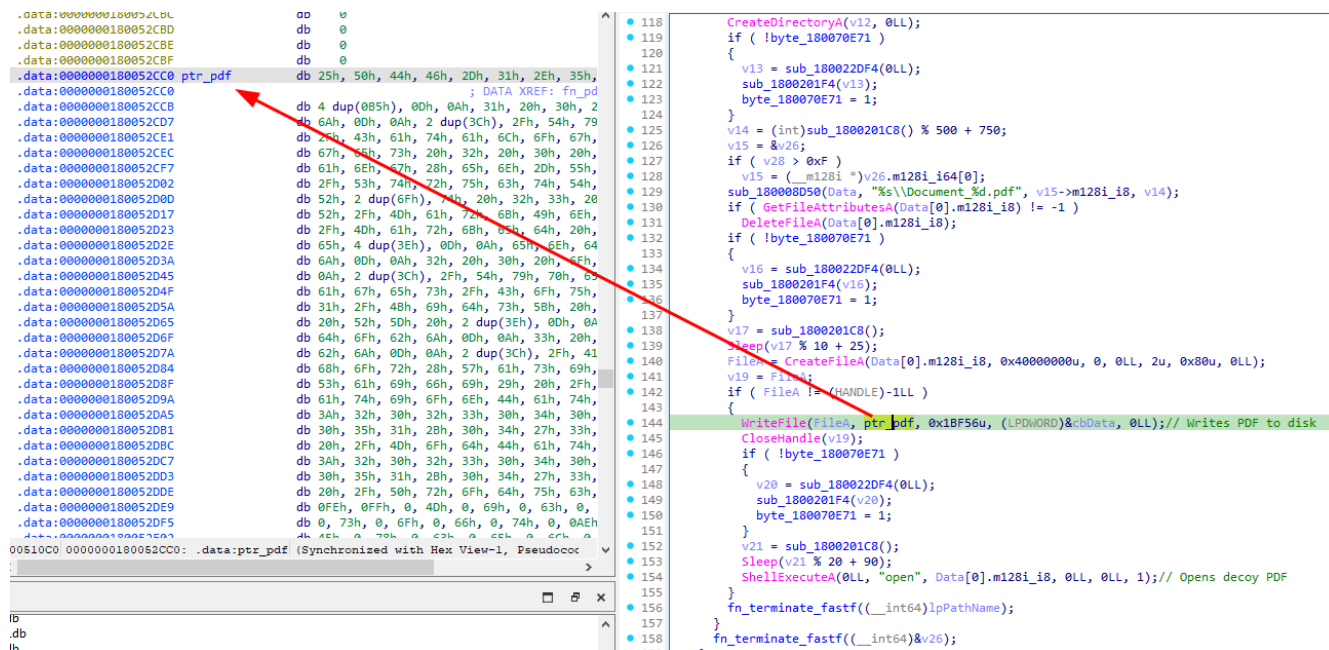


Figure 5: Argument check and execution of embedded PDF.

The embedded dropped PDF is in Pashto and is titled ریاست الوزراء - د دفتر لوی ریاست (machine translation: Office of the Prime Minister - The Office of the Director General - List of Officials). The PDF contains a list of individual names and their corresponding position name, salary, department, and phone number.

 ریاست الوزراء د دفتر لوی ریاست د سیالنه لست						
#	نوم او تخلص	دنده	اداره	د سسکو شمېره	د تلیفون شمېره	کتنې
۱	مول	مرستیال	د سرچینو او ادارې مرستیالې	3801	72 1	
۲	مول	وېاند	د ا.ا.ا. د وېاند دفتر	2021	77 6	
۳	مول	مرستیال	د ا.ا.ا. د وېاند دفتر	2616	70 4	
۴	مول	مرستیال	د ا.ا.ا. د وېاند دفتر	2617	70 1	
۵	مول	مرستیال	د عامه او استراتیژیکو اړیکو مرستیالې	2323	70 5	
۶	مول	رئیس	ریاست دعوت و ارشاد		79 0	
۷	مفتی	رئیس	مرکز اطلاعات و رسانه های حکومت	2600	70 0	
۸	مول	رئیس	ریاست سکرتریت دولتي داری باز	2828	78 7	
۹	مول	رئیس	د مالي ریاست	2533	70 1	
۱۰	مول	رئیس	ریاست مطبوعات	2627	70 5	
۱۱	مول	مرستیال	د تشریفاتو ریاست	2162	78 6	
۱۲	مول	رئیس	د اړیکو او اسنادو ریاست	2425	74 7	
۱۳	مول	رئیس	د ریاست الوزراء د مرستیالاتو سره د همغږۍ ریاست	2447	70 0	
۱۴	مول	رئیس	د سیاسي او ولسي چارو ریاست	2988 / 2422	77 1 / 07 4	
۱۵	مول	رئیس	د کلتوري او ټولنیزو چارو ریاست	2565	70 0	
۱۶	مول	رئیس	د پلانګذاري او مطالعاتو ریاست	2234	70 3	
۱۷	مول	رئیس	د بشري سرچینو ریاست	2174	79 6	
۱۸	مول	رئیس	اداري ریاست	2636	70 8	
۱۹	انج	آمر	آمریت حفظ و مراقبت		74 9	
۲۰	مول	آمر	آمریت خدمات	2800	74 4	
۲۱	مول	آمر	آمریت تخنیک و ترانسپورت	2643	70 1	
۲۲	مول	آمر	آمریت تکنالوژي معلوماتي	2020	70 6	
۲۳	مول	آمر	آمریت تدارکات	2107	79 8	

Figure 6: Decoy PDF.

The backdoor configuration is XOR encrypted with key thisscert23\$SecretKey206. Upon decryption, we obtain the following C2 infrastructure: 185.235.137.35:9000. This IP address is owned by HZ Hosting Ltd.

```

{
    v15[0].m128i_i64[0] = 0x5C5050415D5C5045LL; // encrypted IP address:45505c5d4150505c4501040a6050
    v15[0].m128i_i32[2] = 0xA040145;
    v15[0].m128i_i16[6] = 0x5060;
    xmmword_180070FC0 = 0LL;
    qword_180070FD0 = 0LL;
    *(_QWORD *)&xmmword_180070FC0 = sub_180007090(0xEuLL);
    *((_QWORD *)&xmmword_180070FC0 + 1) = xmmword_180070FC0;
    v1 = xmmword_180070FC0 + 14;
    qword_180070FD0 = xmmword_180070FC0 + 14;
    fn_memcpy_like((__m128i *)&xmmword_180070FC0, v15, 0xEuLL);
    *((_QWORD *)&xmmword_180070FC0 + 1) = v1;
    atexit(sub_18003A860);
    fn_SRW_lock_mutex_2(&dword_180070F78);
}
}
if ( dword_180070F74 > *v0 )
{
    fn_SRW_lock_mutex(&dword_180070F74);
    if ( dword_180070F74 == -1 )
    {
        v15[0].m128i_i32[0] = 0x4359584D; // encrypted port 4d585943. Decrypts to 9000
        xmmword_180070F80 = 0LL;
        qword_180070F90 = 0LL;
        v2 = (_DWORD *)sub_180007090(4uLL);
        *(_QWORD *)&xmmword_180070F80 = v2;
        qword_180070F90 = (__int64)(v2 + 1);
        *v2 = v15[0].m128i_i32[0];
        *((_QWORD *)&xmmword_180070F80 + 1) = v2 + 1;
        atexit(sub_18003A7E0);
        fn_SRW_lock_mutex_2(&dword_180070F74);
    }
}
if ( dword_180070FB0 > *v0 )
{
    fn_SRW_lock_mutex(&dword_180070FB0);
    if ( dword_180070FB0 == -1 )
    {
        qmemcpy(v15, "thisscert23$SecretKey206", 24); // XOR key
        xmmword_180070F98 = 0LL;
        qword_180070FA8 = 0LL;
    }
}

```

Figure 7: Encrypted configuration.

185.235.137.35 • HOST
REMOTE_ACCESS

Summary

Reverse DNS	No Data
Forward DNS	megazonehub.xyz
OS	No Data
2 Total Services	443 / HTTP 56777 / RDP

Network and Routing

Autonomous System	AS59711 (HZ-EU-AS - HZ Hosting Ltd)
Organization	HZ Hosting Ltd 59 Iztochen Blvd. - Kamenitsa Park, 4000, Plovdiv, BULGARIA
Routing Prefix	185.235.137.0/24
WHOIS Network	HZ Hosting Ltd HZ-NA57

Frankfurt am Main, Germany (50.11...)

Netherlands
Belgium
Luxembourg
Paris

© AS OF SEP 17, 2026 | 20:00 UTC

Figure 8: Encrypted configuration.

After decrypting the C2 configuration, the backdoor initiates a connection loop to the C2. The first connection sends a registration beacon with basic system information. The following victim machine details are sent in JSON format:

- `clientId`: Uses the MachineGuid from HKLM\SOFTWARE\Microsoft\Cryptography.
- `machineName`: Uses `GetComputerNameA`.
- `osVersion`: Uses `RtlGetVersion` from `ntdll.dll`.

- `clientId`: Uses a hard-coded value of 1.0.0, suggesting this is one of the first releases of this backdoor.

Sample registration beacon:

```
{
  "clientId": "<MachineGuid>",
  "machineName": "<MachineName>",
  "osVersion": "Windows 10 (Build
X)",
  "clientVersion": "1.0.0"
}
```

The backdoor supports the following 13 commands. The communication with the C2 is mostly in JSON format.

Command	Action
0xA	Send system profile (cpu, memory, disks, network information, uptime)
0x14	Directory and drive listing
0x16	Read files in chunks (download victim -> C2)
0x18	File upload (C2-> victim) as a .tmp
0x19	File write
0x1A	Finalize write, including renaming .tmp to actual extension
0x1B	Process execution, receives path and argument. Uses “cmd.exe /c start” for non-executables
0x1D	Delete file/directory
0x1E	Process listing, retrieves pids, parent process pids, number of threads, working set size, and path
0x20	Process termination by pid (with TerminateProcess)
0x28	Create a shell (Spawns hidden cmd with anonymous pipes)
0x29	Kill the shell

Command	Action
0x2A	Input to shell (raw C2 payload for cmd stdin)

All packets include the 0xDEADBEEF magic number, protocol version, message type, and payload length. The payload is typically JSON, but some commands, like file transfer and shell commands use a mixed binary format containing a JSON header followed by raw binary data.

```

v8 = v2b;
if ( v23 != 0xDEADBEEF || v24 != 1 )
    return 0;
v9 = v26;
v19 = 0LL;
v20 = 0LL;
if ( v26
    00 /* 0x00000000 */ ... 00000000/0000

```

Figure 9: Checks for the 0xDEADBEEF magic number in the code.

```

00000000 ef be ad de 01 00 01 00 92 00 00 00 7b 22 63 6c .....{"c1

```

Figure 10: Sample magic number in a packet.

IOCs

- ZIP file: d69d27a94c78889fc8694e13c122438125eb3d3e6023e0624b3137c7f982a852
- dgxi.dll: a6ceacda670b88e8a8ec9ff5da6a77d9f1c896d6479b2dadb700474a8c408f80
- C2: 185.235.137[.]35:9000