警惕境外APT组织在GitHub投毒，攻击国内安全从业者、指定大企业

原创 微步情报局 微步在线研究响应中心 2025年01月08日 17:04 北京

1 摘要

- 近期网络流传网络安全从业人员使用的某提权工具被植入后门，造成了工具使用者的身份和数据泄露。经微步研判，该事件为东南亚APT组织“海莲花”利用GitHub发布带有木马的Cobalt Strike漏洞利用插件，针对网络安全人员发起的定向攻击。微步情报局已于2024年11月掌握该攻击事件，并已定位到攻击者Github账号。
- 攻击者在此次攻击中首次使用了向Visual Studio工程中投递恶意.suo文件的攻击手法，当受害者编译该Visual Studio工程时，木马会自动执行，攻击方式新颖且隐蔽。
- “海莲花”在近期多个事件中分别针对国内不同行业和人群发起定向攻击，并会定向攻击指定大型科技企业，首次攻击时间在2024年9月中旬至10月初，微步情报局已捕获多个可疑资产及木马文件。
- 微步通过对相关样本、IP 和域名的溯源分析，提取多条相关IOC，可用于威胁情报检测。微步威胁感知平台 TDP 、威胁情报管理平台 TIP 、威胁情报云 API 、云沙箱 S、沙箱分析平台 OneSandbox、互联网安全接入服务 OneDNS 、威胁防御系统 OneSIG 、终端安全管理平台 OneSEC 等均已支持对此次攻击事件的检测与防护。

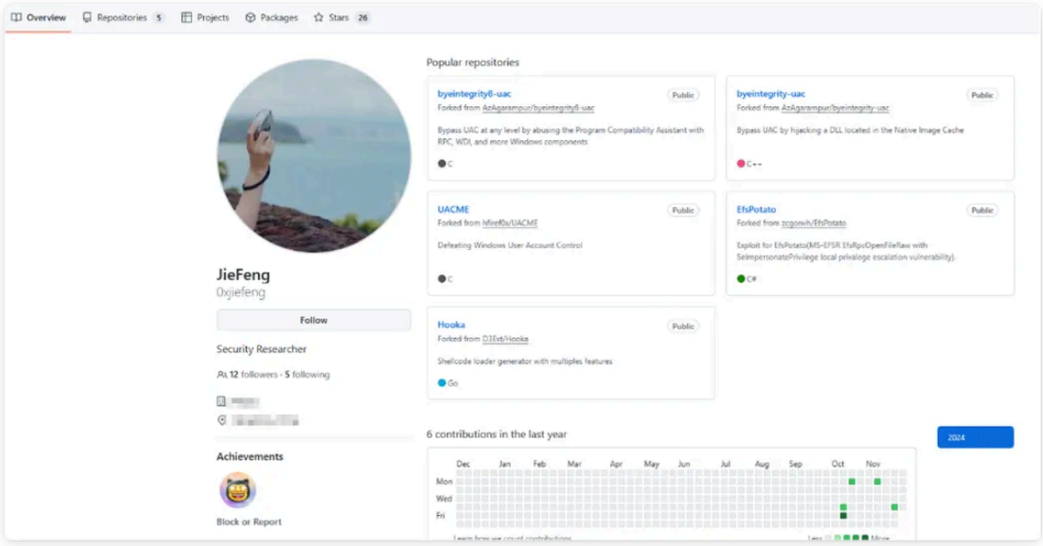
2 事件概要

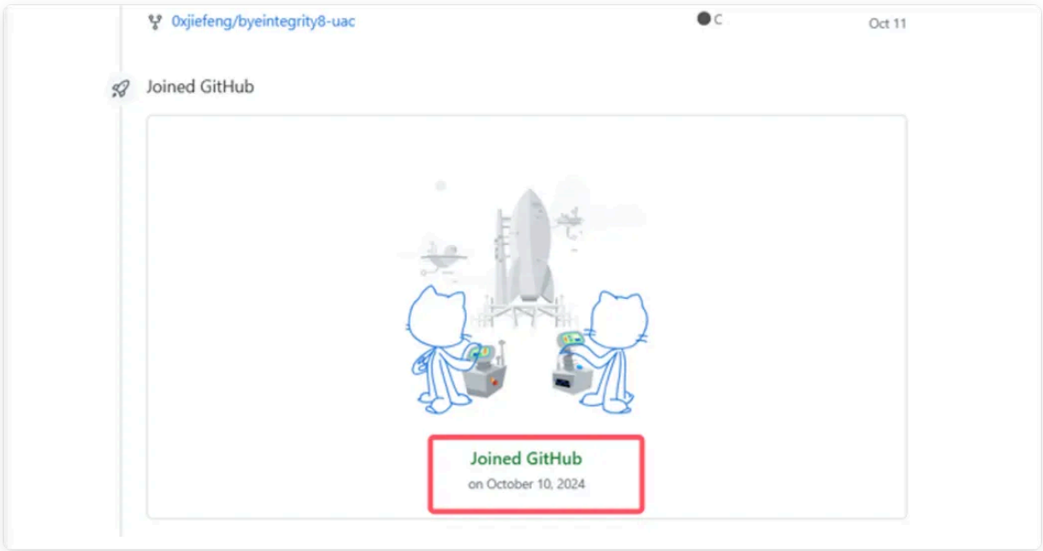
攻击目标	国内安全研究人员
攻击时间	2024年10月中旬
攻击向量	Github投毒
攻击复杂度	中
最终目的	远程控制、情报窃密

3 事件详情

此次“海莲花”攻击的主要手法是在GitHub上发布安全工具开源项目，吸引国内安全相关研究人员下载和二次传播，投毒账号链接：https://github.com/0xjiefeng

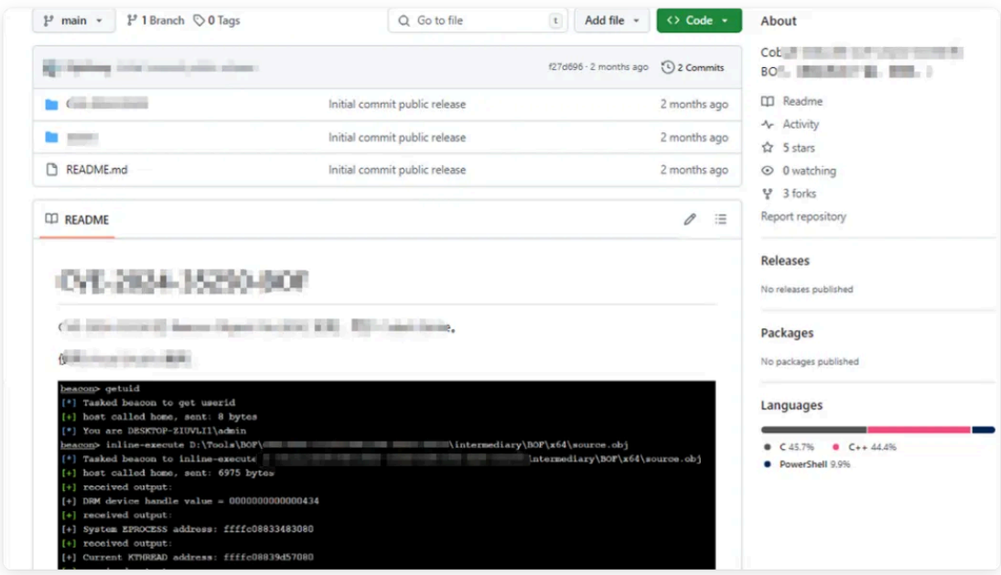
2024年10月10号，攻击者注册该账号，并伪装成国内某头部FinTech公司安全研究员，在主页fork各类安全工具项目来降低受害者戒备心理。

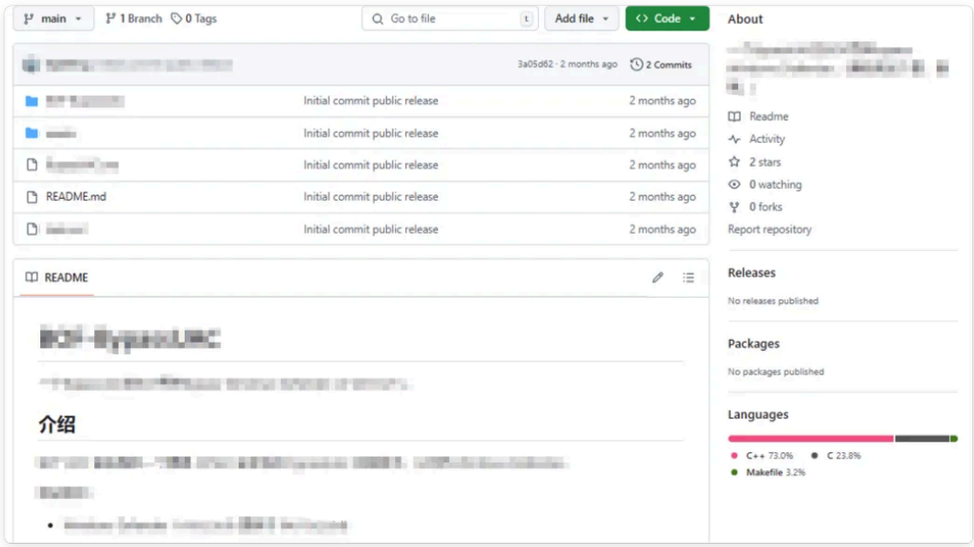




2024年10月14号和10月21号，攻击者共发布两个恶意投毒项目，内容为国内常用红队工具 Cobalt Strike 的插件，包含新的漏洞利用功能，攻击者在项目介绍中使用中文描述，以此来吸引更多的国内安全行业目标人员。

目前攻击者账号已将发布的项目删除，但是相关投毒项目代码已被合并到其他国内安全研究者的存储库中，至今仍可访问。





项目介绍部分的中文表达存在明显的机器翻译痕迹，主要引导目标用户使用Visual Studio打开项目的.sln文件来触发后续恶意代码执行。

当受害者使用Visual Studio打开 .sln 或者.csproj 项目文件后，Visual Studio 会自动加载并调用与之关联的 .suo 文件，从而触发执行其中恶意代码。此次事件中，“海莲花”首次使用了调用.suo文件的攻击手法，恶意代码执行一次即会被覆盖删除，具有极强的隐蔽性。

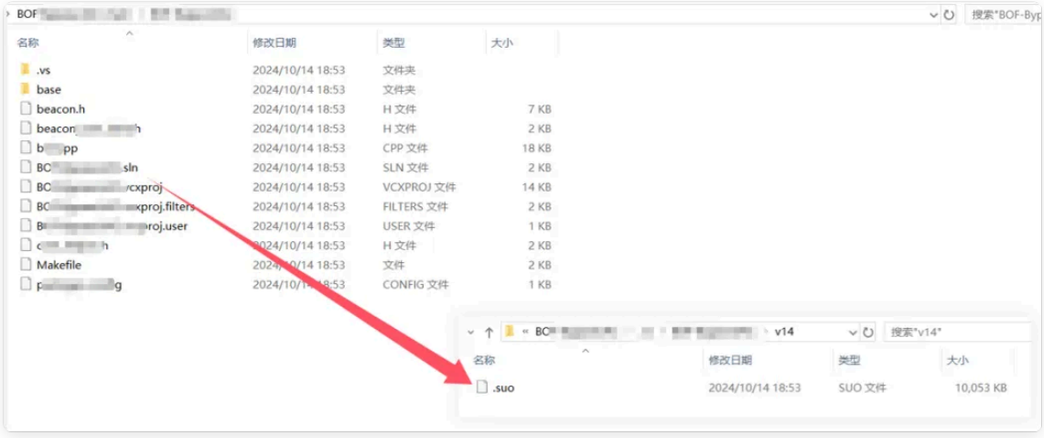
相关的技术概念验证可参考文章：

https://github.com/cjm00n/EvilSln

根据后续分析发现，此次投毒攻击事件在国内安全行业传播范围比较大，国内多家安全相关公众号分享此被投毒项目，存在大量浏览和转发。

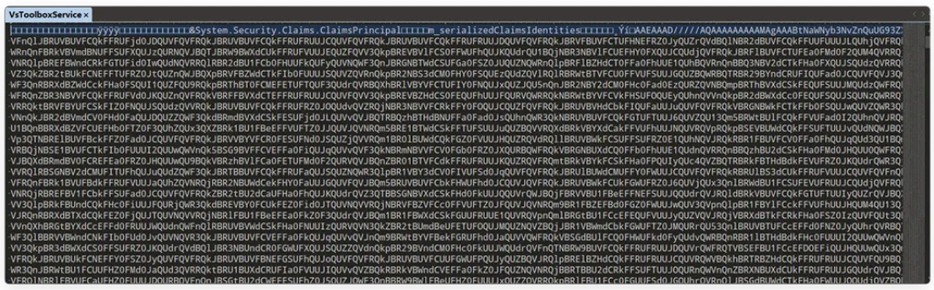
4 关联分析

当目标受害者使用Visual Studio打开项目的解决方案文件（.sln）进行编译时，,Visual Studio会自动加载并调用相关的 .suo（解决方案用户选项）文件，从而触发其中恶意代码执行。并且由于 Visual Studio 在关闭时将新内容保存到 .suo 文件，恶意代码就会被清除，从而使整个攻击行动更难以被发现。



通过加载VSPackage中VsToolboxService流，利用BinaryFormatter 反序列化加载执行其中用base64编码后的恶意代码。

```
// Microsoft.VisualStudio.Toolbox.VsToolboxService
internal void LoadOptions(Stream stream)
{
        BinaryReader binaryReader = new BinaryReader(stream);
        BinaryFormatter binaryFormatter = new BinaryFormatter();
        int num = binaryReader.ReadInt32();
        for (int i = 0; i < num; i++)
        {
                string text = binaryReader.ReadString();
                int num2 = binaryReader.ReadInt32();
                for (int j = 0; j < num2; j++)
                {
                        string text2 = this.Links.Read(stream);
                        VsToolboxService.ToolboxItemContainer toolboxItemContainer = (VsToolboxService.
                        if (text2 != null && File.Exists(text2))
                        {
                                toolboxItemContainer.LinkFile = text2;
                                this.Links.TrackLink(text2);
                                this.Items.GetFilteredList(text).Add(toolboxItemContainer);
                        }
                }
        }
}
```



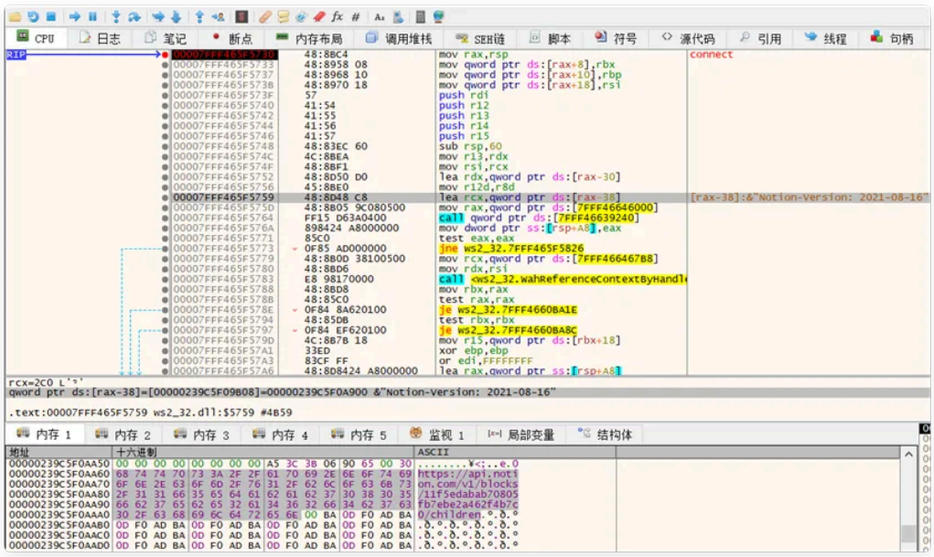
经过样本分析发现，执行项目后会将恶意白加黑组件释放到目录：

C:\Users\Public\TTDIndexerX64\TraceIndexer.exe

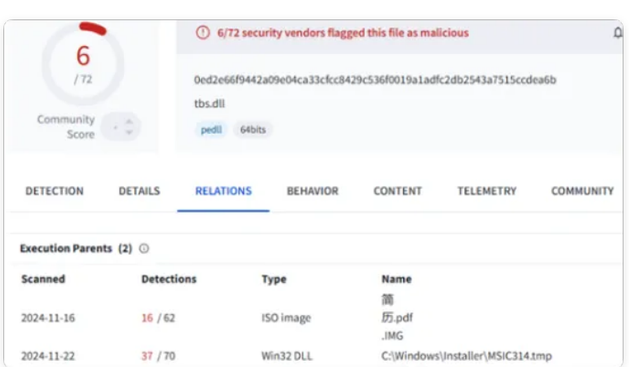
C:\Users\Public\TTDIndexerX64\TTDReplay.dll

并将其写入到自启动注册表：

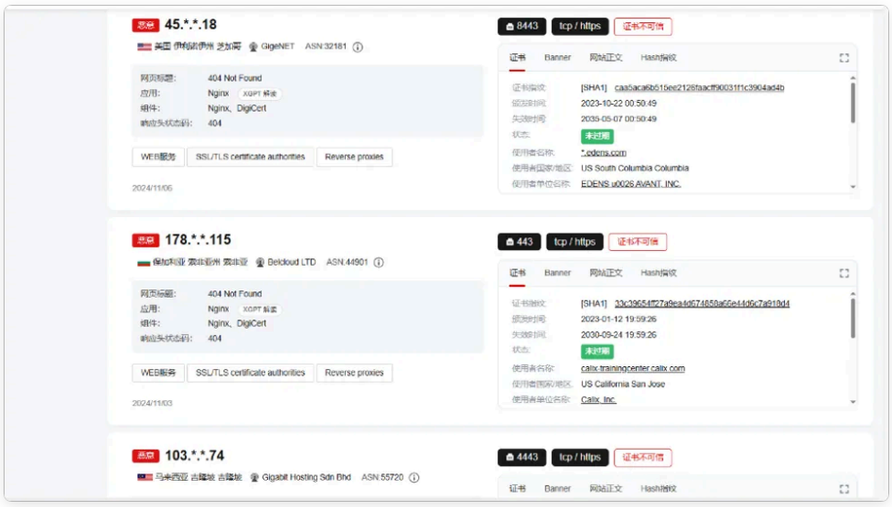
在Shellcode执行方面则是使用到海莲花组织常用dll镂空手法，通过加载系统xpsservices.dll后将其镂空，再把shellcode覆写到该dll的内存空间中执行恶意功能。该程序最终利用国外笔记平台Notion的api来实现c2通信，规避流量检测和拦截，将命令嵌入到 Notion 工作区中实现初始的收发指令。



在样本层面上，根据该样本代码结构、加载方式、元数据、字符串等特征可以关联到更多相似文件，其中关联的样本中“tbs.dll”的父文件则是安全企业披露的海莲花组织以鱼叉邮件攻击国内政企行业样本。



微步测绘数据关联发现，该组织在此攻击活动的资产不仅限于单一的C2资产，攻击资产存在较为显著的端口测绘特征，本次海莲花组织开始活跃攻击时间范围大致在9月中旬到10月初，根据测绘数据以及海莲花本批攻击的样本编译时间判断，在资产部署时间上基本吻合。通过相关的特征检索，还发现了其他活跃的可疑线索C2地址。



在分析同批攻击样本时发现，海莲花此次攻击目的性较强，部分样本在执行过程中会检测受害者计算机名和目标是否一致，来定向攻击特定大型科技企业用户。

```
1  __int64 __fastcall sub_1400E9E50()
2  {
3    unsigned int v0; // esi
4    char String1[16]; // [rsp+30h] [rbp-40h] BYREF
5    char *String2; // [rsp+40h] [rbp-30h] BYREF
6    __int64 v4; // [rsp+50h] [rbp-20h] BYREF
7
8    sub_14002CE90(&String2);
9    strcpy(String1, "[redacted]U");
10   LOBYTE(v0) = strcmpi(String1, String2) != 0;
11   if ( String2 != (char *)&v4 )
12     j_j_free_2(String2);
13   return v0;
14 }
```

```
sub_1000ABC0(&String2);
strcpy(String1, "D[redacted]Q");
v0 = strcmpi(String1, String2);
LOBYTE(v0) = v0 != 0;
v1 = v0;
if ( String2 != (char *)&v5 )
  j_j_free(String2);
return v1;
```

附录-IOC

回连Notion的page_id：

11f5edabab708090b982d1fe423f2c0b

相关海莲花攻击C2：

190.211.254.203:4443

45.41.204.18:8443

45.41.204.15:443

178.255.220.115:443

103.91.67.74:4443

154.93.37.106:443

193.138.195.192:8443

38.54.59.112:80

- END -

#威胁通告 127 # 安全报告 126

威胁通告 · 目录 ≡

< 上一篇 · 漏洞通告 | Windows 轻量级目录访问协议 (LDAP) 拒绝服务漏洞