1024041137 张宇昊的绘图作业

ELASTIC规则关系图

ggggugeliulanqGoogle1217.msi

安装释放

c:\users\public\documents\

Google.exe

启动

c:\users\public\documents\Main\current\

log2.dll ←加载→ DingTalk.exe →加载→ DataReport.dll →释放并执行→ FANG.bat

c:\users\public\documents\Main\current\WindowsData\

me.key ←解压→ kail.exe ←调用→

释放

真正的chrome安装包   setup.exe

导出函数:shellex

最终载荷

加载后调用→ Server.dll

NtHandleCallback.exe

载入

反射式加载

Irrlicht.dll ←载入并解密→

加载后调用→ Install.dat ←解密并反射式加载→ server.log

导出函数：NtHandleCallback

WindowsPowerShell WbemScripting.SWbemLocator.vbe

启动

移动到启动目录

```powershell
1    # 输入文件路径
2    $inputFile = "./clsids.txt"
3
4    # 输出文件路径
5    $outputFile = "./ShellMethodsResult.txt"
6    $outputFile1 = "./Result.txt"
7    # 确保输出文件为空
8    Set-Content -Path $outputFile -Value ""
9
10   # 读取 CLSID 文档中的所有行
11   $clsidList = Get-Content -Path $inputFile
12
13   # 遍历每个 CLSID
14   foreach ($clsid in $clsidList) {
15       try {
16           # 去掉空白字符
17           $clsid = $clsid.Trim()
18
19           # 检查 CLSID 是否有效
20           if ([string]::IsNullOrWhiteSpace($clsid)) {
21               continue
22           }
23           Write-Host "Processing CLSID: $clsid"
24           # 尝试创建实例
25           $instance = [Activator]::CreateInstance([type]::GetTypeFromCLSID($clsid))
26
27           # 如果实例成功，检查与 shell 相关的方法
28           if ($instance -ne $null) {
29               $methods = $instance | Get-Member -MemberType Method | Where-Object { $_.Name -like "*launch*" }
```
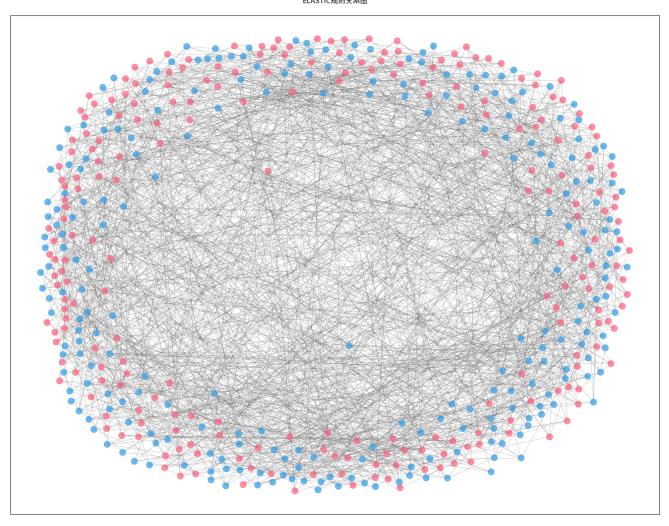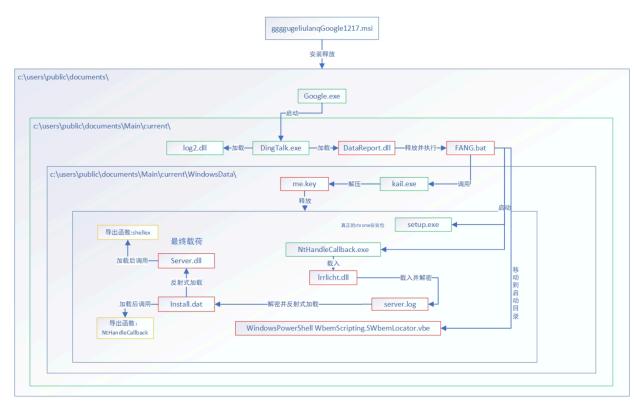
```
Processing CLSID: {FF2A742B-CA25-4507-BD93-6BA9B8E8965F}
Processing CLSID: {FF2AB3A5-5EBA-4538-8F8F-C169CCD40200}
Processing CLSID: {FF2F95A4-C6A1-4B48-BC87-8709250E0D03}
Processing CLSID: {FF302BD3-3DC6-4680-9384-621A7FF574F4}
Processing CLSID: {ff363bfe-4941-4179-a81c-f3f1ca72d820}
Processing CLSID: {FF393560-C2A7-11CF-BFF4-444553540000}
Processing CLSID: {FF3AE31D-55B0-4945-BDE9-622ABB334C1A}
Processing CLSID: {ff48dba4-60ef-4201-aa87-54103eef594e}
Processing CLSID: {FF51D680-9190-4B6C-87DA-0062ABBBFF2E}
Processing CLSID: {FF5265E8-6D8B-4BD4-A52D-8D99008B04C8}
Processing CLSID: {ff609cc7-d34d-4049-a1aa-2293517ffcc6}
Processing CLSID: {ff679da1-8ff2-4474-9c9e-52bbd409b557}
Processing CLSID: {FF806D42-727C-4663-A497-A898FAE3C637}
Processing CLSID: {ff89cdc6-6535-49df-8c70-19ea5acd4948}
Processing CLSID: {ff8a32e3-a9a7-4093-b9c4-5b5b4f30ab63}
Processing CLSID: {ff8a71c2-7eb8-418b-950d-3b49f43f024f}
Processing CLSID: {FF97298A-DE83-4D65-84EA-821C06206C47}
Processing CLSID: {FF99E1C1-7F9A-4C83-8A57-305992EDD07B}
Processing CLSID: {ff9e6131-a8c1-4188-aa03-82e9f10a05a8}
Processing CLSID: {FFB8655F-81B9-4fce-B89C-9A6BA76D13E7}
Processing CLSID: {FFC9F9AE-E87A-3252-8E25-B22423A40065}
Processing CLSID: {FFCDB781-D71C-4D10-BD5F-0492BAFFD90A}
Processing CLSID: {FFCECE86-332F-49B4-B9EE-7FECEFAD3E10}
Processing CLSID: {ffd90217-f7c2-4434-9ee1-6f1b530db20f}
Processing CLSID: {ffe1df5f-9f06-46d3-af27-f1fc10d63892}
Processing CLSID: {FFE1E5FE-F1F0-48C8-953E-72BA272F2744}
Processing CLSID: {FFE2A43C-56B9-4bf5-9A79-CC6D4285608A}
Processing CLSID: {FFB8C349-2BB1-411F-93CB-0364C5F9FD9F}
处理完成，结果已保存到 ./ShellMethodsResult.txt

PS C:\Users\master>
```