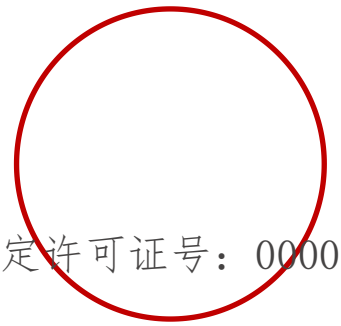
510321200000 鉴定检验报告书



司法鉴定许可证号：000000000

声　　明

1、委托人应当向鉴定机构提供真实、完整、充分的鉴定材料，并对鉴定材料的真实性、合法性负责。

2、司法鉴定人按照法律、法规和规章规定的方式、方法和步骤，遵守和采用相关技术标准和技术规范进行鉴定。

3、司法鉴定实行鉴定人负责制度。司法鉴定人依法独立、客观、公正地进行鉴定，不受任何个人和组织的非法干预。

4、使用本鉴定文书应当保持其完整性和严肃性。

地址：510321200000

联系电话：000-00000000

司法鉴定意见书

510321200000 司法鉴定中心[2023]电检字第 1 号

一、基本情况

委 托 人：××市公安局××支

委托鉴定事项：对受害人台式机内提取的木马文件 artifact.exe 进行功能性鉴定。

受理日期：2023 年 6 月 7 日

鉴定材料：受害人台式机内提取的木马文件 artifact.exe。

鉴定日期：2023 年 6 月 8 日

鉴定地点：510321200000 取证实验室

在场人员：黄 X、徐 XX、漆 X

二、检案摘要

鉴定委托书记载：2023 年 5 月 29 日，黑客先入侵了某政府媒体网站，并对局域网电脑进行了内网渗透，进入某大运会宣传主编的台式机内，并在该主编的台式机内上传了一段反党视频。通过现场取证已获得受害人台式机镜像 1 份，在该镜像内发现一木马文件 artifact.exe。

三、检验过程

1.鉴定设备及软件：美亚柏科取证航母 FL-2000、微步云沙箱在线版、Chrome（版本：114.0.5735.110）、火绒杀毒软件（版本：5.0.73.6）。

2.电子数据取证标准：

1)国家标准：电子物证数据搜索检验规程（GB/T 29362-2012）。

2)公共安全行业标准：法庭科学电子数据收集提取技术规范（GA/T 756-2021）；电子数据法庭科学鉴定通用方法(GA/T 976-2012)；程序功能检验方法（GA/T 757-2008）。

3)技术规范：电子数据司法鉴定通用实施规范（SF/Z JD0400001-2014）；电子数据复制设备鉴定实施规范（SF／Z JD0401001-2014）。

3.鉴定方法：

1)证据数据提取固定:通过程序功能检验方法对涉案木马的功能进行检验，并记录检验结果。

2)证据数据检验分析:对鉴定过程取得的检验结果作为鉴定结果的数据源，并记录录屏文件的哈希值。

4.鉴定过程：

1)准备鉴定环境：

使用火绒杀毒软件对取证航母进行快速扫描，未发现病毒，同时对检验工作站及周边环境进行了防磁、防水、防静电和防震保护。

2)检验开始时间：在检验工作站通过 ping 百度获取检验开始时间为 2023 年 06 月 09 日 10:47:51。部分操作如图 1 所示：

图 1

3)使用谷歌浏览器（Chrome）登录微步云沙箱网站 https://s.threatbook.com，点击提交文件后将该木马文件上传至微步云沙箱进行分析。部分页面如图 2 所示。

图 2

通过分析，该木马具有远程控制功能，远程控制 IP 地址为 118.24.75.245。部分内容页面如图 3 所示。

图 3

通过对该木马进行行为检测，该木马有 CobaltStrike 命名管道特征。在 CobaltStrike 中，Beacon 是其核心组件之一。Beacon 是一种轻量级的恶意软件代理工具，用于与受感染的目标系统建立 C2 通信通道，并与攻击者的 C2 服务器进行交互。Beacon 旨在实现持久化访问、命令执行和数据传输等功能，以支持攻击者远程控制受感染系统，并执行各种攻击行动。部分内容页面如图 4 所示。

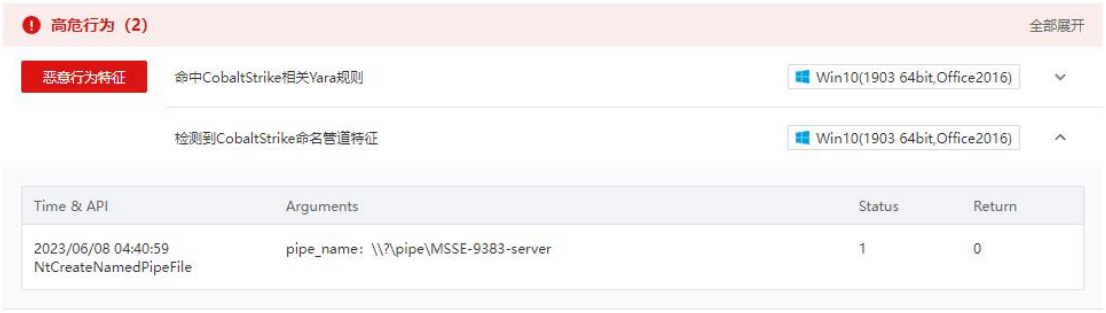


图 4

该木马还具有使用 UPX 进行压缩、传输恶意流量、创建 shellcode 以及将将可读可写的内存属性改为可读可执行的功能。部分内容页面如图 5 所示。

图 5

四、检验结果

对送检的木马文件 artifact.exe 进行功能性检验，鉴定意见如下：

1. 通过对该木马文件进行分析判定，该木马文件属于=CobaltStrike 木马家族。

2. 该木马文件具有远程控制功能,远程控制 IP 为 118.24.75.245。

司法鉴定人签名或者盖章

《司法鉴定人执业证》证号：

司法鉴定人签名或者盖章

《司法鉴定人执业证》证号：

（司法鉴定机构司法鉴定专用章）

二〇二三年六月九日

（文书制作日期：用简体汉字将年、月、日标全，“零”写为“〇”，居右排列。日期处加盖司法鉴定机构的司法鉴定专用章红印）