

瞄准微信、钉钉等工具定向投放远控木马|游蛇（银狐）技战术追踪

 antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202512.html

安天

1.概述

“游蛇”团伙很可能在以欺诈即服务（FaaS，Fraud as a Service）的网络犯罪模式运营，以商品化并按需出售或租赁的形式，向其他犯罪分子提供攻击方法、工具、基础设施，从而大幅降低实施网络欺诈的门槛。

2.技术梳理

2.1 谷歌搜索引擎SEO技术投毒

图2-1 谷歌搜索引擎结果

图2-2 仿冒“百度网盘”的恶意网站

2.2 样本执行流程

样本运行后同时投放并启动了一个正常的百度网盘安装程序和一个恶意载荷。恶意载荷通过系统自带程序rundll32.exe加载并执行恶意DLL。该DLL会读取同目录下的加密文件并解密，生成并启动第一组木马，其会连接C2服务器202.95.16.100:80。随后该组件从C2下载一组恶意模块，该模块对系统进程进行扫描（包括WeChat（微信）、DingTalk（钉钉）、Telegram、WhatsApp等即时通讯进程）。若发现上述任意进程，模块会在%APPDATA%\Embarcadero下创建一个标记文件。检测到该标记文件后，攻击者利用系统进程regsvr32.exe重新执行恶意DLL，使其解密/下载并部署Winos远控木马，该木马会连接C2服务器27.124.45.66:80。整体组件涉及多个加密组件利用解密、内存加载、关闭安全软件网络连接等方式规避检测。

图2-3 样本执行流程图

3.样本分析

3.1 初始诱饵文件及文件功能概览

表3-1样本标签

病毒名称	Trojan/Win32.SwimSnake
------	------------------------

原始文件名	Baidu-2025102902.exe
MD5	D56FDF251110FBAD9064DA33CDD51E54
处理器架构	AMD64
文件大小	501.15 MB (525,494,999字节)
文件格式	Win32 EXE
时间戳	伪造
数字签名	无
加壳类型	无
安装程序	Install Builder

Baidu-2025102902.exe运行后会将正常的“百度网盘安装软件”安装包释放至C:\Program Files目录下并执行安装程序，在桌面上创建快捷方式，并在多个系统安装路径中释放多组恶意载荷，用于后续从中选择攻击载荷。

此次样本涉及的核心组件及功能描述如下表所示：

表3-2 文件及功能描述

文件名称	功能
xmplay.exe	规避检测：NSIS打包的加载器，用来释放和执行后续恶意样本，利用PowerShell命令将指定盘符加入Defender的排除列表
Verifier.exe	shellcode加载器，对同目录下的Profiler.json文件进行解密得到一段shellcode，第二次解密得到Single.dll
Profiler.json	

Single.dll	规避检测：提权，修改TCP连接表，切断安全软件进程与其远程服务器的网络通信
AutoRecoverDat.dll	shellcode加载器，对同目录下GPUCache.xml和GPUCache2.xml进行解密
GPUCache.xml	
GPUCache2.xml	
APTBIN_Main.dll	创建计划任务、连接C2服务器202.95.16.100:18852下载VFPower_32.dll文件
VFPower_32.dll	连接C2服务器202.95.16.100:80下载UserInfoPlugin.dll文件，与C2服务器建立心跳
UserInfoPlugin.dll	收集系统信息，对当前系统IM应用进行检测，如果发现IM应用，会利用regsvr32.exe程序重新执行AutoRecoverDat.dll，该dll会读取GPUCache2.xml进行解密得到Code_Shellcode后门.dll
Code_Shellcode后门.dll	内存加载器，连接第二个C2服务器27.124.45.66:443下载上线模块.dll
上线模块.dll	利用配置信息轮询连接C2地址27.124.45.66，端口号为80、58600、1433，与C2服务器建立心跳
登录模块.dll	键盘记录、剪贴板监控、屏幕截图等基本功能，并支持接收执行多种远控命令。

3.2 样本分析

3.2.1 初始投放恶意载荷分析

初始投放恶意载荷样本使用Install Builder工具进行打包。该载荷创建于2025年11月19日。

图3-1 使用InstallBuilder工具进行打包

该初始恶意载荷的功能是将正常的百度网盘安装包释放到C:\Program Files，将恶意载荷xmplay.exe释放到用户目录下，创建百度网盘的快捷方式并执行其安装包程序，最后执行主恶意载荷xmplay.exe。

图3-2 执行恶意载荷

3.2.2 第二层载荷分析

xmplay.exe恶意载荷实际上是NSIS打包程序，里面存放了多个恶意文件。首先启动时执行PowerShell命令将指定盘符加入Defender的系统防护排除列表，为恶意程序进入系统放行，从而降低用户系统的安全防护能力。

图3-3 利用PowerShell命令降低防护

之后将多个加密数据文件从TEMP目录复制到系统路径，如下表所示。

表3-3 加密数据替换到系统路径

TEMP目录下文件	系统路径
temp_k.txt	%LOCALAPPDATA%\Temp\temp_k.txt
lic.dat	%LOCALAPPDATA%\Verifier.exe
Profilerjson	%LOCALAPPDATA%\Profiler.json
GPUCachexml	%APPDATA%\Embarcadero\GPUCache.xml %APPDATA%\GPUCache.xml
GPUCache2xml	%APPDATA%\Embarcadero\GPUCache2.xml %APPDATA%\GPUCache2.xml
Auto.dat	%APPDATA%\Embarcadero\AutoRecoverDat.dll
miuahfzc	%LOCALAPPDATA%\miuahfzc
zwa	%LOCALAPPDATA%\zwa

用xmplay.exe恶意载荷中的DcryptDll.dll解密上述文件并生成恶意组件，用nsExec.dll执行cmd指令。首先执行第一个恶意组件Verifier.exe（Shellcode加载），然后通过系统自带的rundll32.exe执行恶意组件AutoRecoverDat.dll。

图3-4 首次执行恶意组件AutoRecoverDat.dll

3.2.3 Shellcode加载与解密

恶意组件Verifier.exe首先会读取同目录下的Profiler.json文件并解密为shellcode。

图3-5 读取Profiler.json文件并解密为shellcode

然后再将shellcode进行二次解密得到Single.dll文件。

图3-6 二次解密得到Single.dll

阻断安全软件网络连接

Single.dll文件会遍历指定安全软件进程，循环枚举安全软件的TCP连接表，切断安全软件进程与其远程服务器的网络通信，以便规避防护。

图3-7 阻断安全软件网络连接

3.2.4 第一组木马程序分析

第二层载荷xmplay.exe首次会使用cmd.exe调用rundll32.exe系统文件执行AutoRecoverDat.dll文件，解密得到shellcode，然后经过二次解密得到APTBIN_Main.dll文件，最终注入到rundll32.exe内存中执行。

图3-8 二次解密得到APTBIN_Main.dll

下载远控木马组件

APTBIN_Main.dll会创建两个线程，功能是结束安全软件进程以及创建计划任务等。之后则连接C2服务器202.95.16.100:18852下载VFPower_32.dll文件。

创建计划任务

创建两个计划任务分别登录执行AutoRecoverDat.dll和Verifier.exe载荷进行shellcode加载。

图3-10 创建计划任务执行恶意文件

连接C2服务器

下载的VFPower_32.dll文件会连接C2服务器地址202.95.16.100:80，下载UserInfoPlugin.dll文件（收集系统信息与精准投放远控），并使用“YourSharedSecretKey”字符串作为心跳包内容。

图3-11 连接C2服务器

收集信息下载Winos远控木马

UserInfoPlugin.dll会收集大量系统、用户、已安装应用及权限相关信息，并对系统中是否运行特定即时通讯进程（微信、钉钉、Telegram、WhatsApp等）进行检测。若发现上述任意进程，组件会在特定目录下创建一个标记文件。监测到该标记文件后，攻击链利用系统进程regsvr32.exe执行AutoRecoverDat.dll，该DLL解密生成名为“Code_Shellcode后门.dll”的模块并从C2下载Winos远控木马，随后将Winos注入到系统regsvr32.exe进程内运行。

遍历并结束安全进程

遍历进程检测如下安全软件进程名，结束当前表中存在的进程。

表3-4 安全软件及相关进程名

3.2.5 Winos远控木马分析

释放的Code_Shellcode后门.dll实际上是内存加载器，主要功能是连接到远程主机（27.124.45.66:443），接收Winos远控木马“上线模块.dll”并执行。

上线模块利用配置信息连接C2地址

Winos远控木马的上线模块中含有配置信息，包括首选及备用的C2地址和端口、分组、版本号、是否启用某项功能等，会根据配置信息轮询连接C2地址下载“登录模块.dll”并建立心跳。

图3-14 上线模块中的配置信息

检查安全分析工具并结束

登录模块会创建一个线程，尝试登录到远控服务器（27.124.45.66）。该dll具备键盘记录、剪贴板监控、屏幕截图等基本功能，并支持接收执行多种远控命令。还会检查每个可见窗口标题是否包含一系列“监控/分析/安全”等工具名称并结束。

图3-15 检查安全分析工具并结束

4.使用工具排查“游蛇”威胁

图4-2 “游蛇”专项排查工具发现被注入远控木马的恶意进程

智甲可对本地磁盘进行实时监测，对新增文件自动化进行病毒检测，对发现病毒可在其落地时第一时间发送告警并进行处置，避免恶意代码启动。例如本次事件中，当恶意文件Single.dll恶意文件落地时，智甲会立即进行告警并清除恶意文件。

图5-1 发现病毒时立即告警

此外，智甲的主动防御能力会实时监控本地进程行为，针对异常文件释放、文件操作、命令执行、异常行为、网络行为等进行监测与分析，一旦发现高风险行为立即拦截。本次事件中，当xmplay.exe向敏感目录释放文件时，智甲会立即告警。

图5-2 发现异常行为时立即拦截

智甲还具有内存防护能力，可实时监控内存环境，可对内存中数据进行检测，并可对异常内存操作进行拦截。本次事件中，当文件Verifier.exe执行shellcode时，智甲可立即拦截。

图5-3 发现内存中恶意代码立即查杀

图5-4 对下载的异常安装包发送风险预警

6.loCs

baiduwangpan[.]cc
https://sen.s-ed1.cloud.gcore.lu/Baidu-2025102902[.]zip
202.95.16[.]100
27.124.45[.]66
D56FDF251110FBAD9064DA33CDD51E54
821E5293B5815F35E9BA9A9E4B93F858
9147C33F1F46151389EEDB5F29CA800A
67E41CB7C6D1A5C891A4CF0BA974929C

4A955BF9245FFECC34A1D3698438BF15
15E01F2C420720F1534C1168E01F2541
7CE0EAE4DB7930357DBDF9A34FEBFEF4
A49A6F85F7E638A2BD1580C78203B49A
D7E3FC5162E22DFD62670A845426298E
D9FEECFDB4B4F5663BDBC8EA395A9E81
9B2919C90ECCDB4B9D1A0B5D4FCE790D
1854962AD353F485E314F60881B7F9CB

[1] 通过伪造中文版Telegram网站投放远控木马的攻击活动分析 [R/OL].(2022-10-24)

https://www.antiy.cn/research/notice&report/research_report/20221024.html

[2] 利用云笔记平台投递远控木马的攻击活动分析 [R/OL].(2023-03-24)

https://www.antiy.cn/research/notice&report/research_report/20230324.html

[3] 利用云笔记平台投递远控木马的黑产团伙分析 [R/OL].(2023-03-30)

https://www.antiy.cn/research/notice&report/research_report/20230330.html

[4] “游蛇”黑产团伙针对国内用户发起的大规模攻击活动分析 [R/OL].(2023-05-18)

https://www.antiy.cn/research/notice&report/research_report/20230518.html

[5] “游蛇”黑产团伙近期钓鱼攻击活动分析 [R/OL].(2023-07-11)

https://www.antiy.cn/research/notice&report/research_report/TrojanControl_Analysis.html

[6] “游蛇”黑产团伙利用微信传播恶意代码的活动分析 [R/OL].(2023-08-22)

https://www.antiy.cn/research/notice&report/research_report/SnakeTrojans_Analysis.html

[7] “游蛇”黑产团伙专题分析报告 [R/OL].(2023-10-12)

https://www.antiy.cn/research/notice&report/research_report/SwimSnakeTrojans_Analysis.html

[8] “游蛇”黑产团伙针对财务人员及电商客服的新一轮攻击活动分析 [R/OL].(2023-11-11)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis.html

[9] “游蛇”黑产近期攻击活动分析 [R/OL].(2024-04-07)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202404.html

[10] “游蛇”黑产团伙利用恶意文档进行钓鱼攻击活动分析 [R/OL].(2024-06-21)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202406.html

[11] 钓鱼下载网站传播“游蛇”威胁，恶意安装程序暗藏远控木马 [R/OL].(2024-12-20)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202412.html

[12] “游蛇”黑产攻击肆虐，速启专项排查与处置 [R/OL].(2025-04-23)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202504.html

[13] “游蛇”黑产利用仿冒的WPS Office下载站传播远控木马 [R/OL].(2025-05-15)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202505.html

[14] “游蛇（银狐）”黑产最新变种攻击活动 [R/OL].(2025-08-17)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202508.html

[15] 游蛇（银狐）黑产传播与技战术持续追踪：仿冒FinalShell管理软件的攻击手法分析动 [R/OL].(2025-09-19)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202509.html

[16] “游蛇（银狐）”黑产密集仿冒各类流行应用：WPS下载站打假专辑 [R/OL].(2025-10-10)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202510.html

[17] 收到此类文件立刻删除！避免落入“游蛇”圈套 [R/OL].(2025-10-23)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Report_202510.html

[18] 多层隐匿载荷解密与驱动级致盲对抗手法分析 | 游蛇（银狐）技战术追踪 [R/OL].(2025-11-20)

https://www.antiy.cn/research/notice&report/research_report/SwimSnake_Analysis_202511.html