

【天穹】HVV专题：典型HVV样本总结与IOC收集（第三期）

mp.weixin.qq.com/s

星图实验室



一、概述

HVV 期间，天穹团队持续推进样本分析工作，依托多引擎动态分析与攻击链还原技术，对狩猎发现的样本开展深度分析。结合本期捕获的典型样本及平台监测数据，发现攻击样本进一步呈现出**诱饵主题定制化、载荷内存化及检测规避技术融合**等特点：样本以“个人简历”“领域专家”等主题作为诱饵，执行后通过 Donutloader、内存注入等方式加载恶意代码，减少恶意载荷在磁盘上的暴露；并结合反调试、反沙箱、关键系统函数覆写等手段规避安全检测，降低 EDR、ETW、AMSI 等安全机制的检测能力，从而提升恶意载荷的隐蔽执行能力，增强对安全分析与监控机制的对抗能力。

天穹沙箱温馨提示：若您收到可疑链接或文件，切勿直接点击或运行！可优先投递至奇安信天穹沙箱进行风险鉴定，通过专业的动态行为检测与威胁情报匹配，精准识别潜在安全风险。使用天穹沙箱过程中，如您遇到任何问题（如样本投递失败、分析结果存疑等），可随时联系我们，我们将第一时间为您提供技术支持与解答。

二、典型样本分析

样本一

- 样本名：固态电池领域专家-郭x-xx大学-xx公司.exe
- MD5：a6d9c3fe61feaa231d1d103ee53527d0

- 文件类型：exe
- C2：

[https://nd-cohen.cn.cdn.dnsv1\[.\]com/sw.js](https://nd-cohen.cn.cdn.dnsv1[.]com/sw.js)

[https://111.6.166\[.\]81/sw.js](https://111.6.166[.]81/sw.js)[https://111.8.3\[.\]214/sw.js](https://111.8.3[.]214/sw.js)[https://112.46.50\[.\]58/sw.js](https://112.46.50[.]58/sw.js)[https://113.142.216\[.\]56/sw.js](https://113.142.216[.]56/sw.js)[https://116.153.4\[.\]140/sw.js](https://116.153.4[.]140/sw.js)[https://116.163.31\[.\]213/sw.js](https://116.163.31[.]213/sw.js)[https://116.163.31\[.\]218/sw.js](https://116.163.31[.]218/sw.js)[https://117.187.145\[.\]123/sw.js](https://117.187.145[.]123/sw.js)[https://119.0.110\[.\]63/sw.js](https://119.0.110[.]63/sw.js)[https://120.222.189\[.\]193/sw.js](https://120.222.189[.]193/sw.js)

报告链接：<https://sandbox.qianxin.com/tq/report/toNewReport.do?rid=3880b67f65cb041da40c33a69e926996&sk=02440341>

- 描述：该样本伪装为 Word 简历文档，运行后首先检测沙箱环境，并通过覆写 ntdll.dll 规避安全监控，随后解密载荷并注入执行，最终加载 CobaltStrike 远控并与 C2 建立通信。
 - 反调试/反沙箱
 - 1) 调试器检测：检查 PEB 中的 BeingDebugged 标志位，当标志位被置位时，判定进程正被调试。
 - 2) 物理内存检测：调用 GlobalMemoryStatusEx 获取物理内存大小，当内存小于约 1GB (0x400FFFFFF) 时，判定可能处于沙箱或虚拟化环境。
 - 3) CPU 核心数检测：调用 GetSystemInfo 获取 CPU 核心数，当 dwNumberOfProcessors 小于等于 1 时，判定可能处于分析环境。
 - 4) 时间差检测：通过两次调用 GetTickCount 计算时间间隔，在执行约 500 ms 的睡眠操作后进行时间校验；若实际时间差小于等于 449 ms (0x1C1)，则判定系统可能存在时间加速或沙箱模拟行为。
 - 覆写 ntdll.dll 代码段：样本打开磁盘上 ntdll.dll 的文件句柄，创建只读映射视图后定位到 .text 节区。随后调用 VirtualProtect 将内存中 ntdll.dll 对应区域改为可写，并将磁盘上的原始字节复制回内存，从而恢复 ntdll.dll 的原始代码，如图 1 所示。这种 Unhook 技术主要用于清除 EDR/AV 在系统 DLL 上设置的 API Hook，恢复相关 API 的原始实现，让 EDR 和杀软更难发现异常行为。

- 图1 NTDLL .text 段覆写

注入并执行解密的载荷

：样本首先对内嵌载荷进行 AES 解密，并通过内存注入方式加载解密后的代码。载荷执行采用主备双执行路径，结合多层执行掩护机制，提高恶意代码执行的成功率，如图 2 所示。

1) 主执行路径：滥用系统组件回调机制，利用 CertEnumSystemStoreW 合法 API 的调用链间接触发恶意代码执行，使载荷执行行为混入正常系统调用流程。

2) 备执行路径：如果上述回调链执行失败，则调用 CreateThread 创建线程，直接执行解密后的载荷，作为主执行路径的兜底机制。

3) 执行掩护机制：

定时器回调与线程上下文篡改（调用栈伪装）：通过 CreateTimerQueueTimer 注册周期性回调，在回调过程中挂起自身工作线程，临时将其 RIP 修改为指向 kernel32!BaseThreadInitThunk，约 50 ms 后恢复原始 RIP 并继续执行，用于掩护正在运行的 Shellcode 线程。

WH_CBT 钩子伪装 Word 弹窗：样本注册线程级 WH_CBT 钩子后弹出“Microsoft Word”错误对话框，在对话框激活时，通过钩子回调替换窗口图标为伪造的 Word 图标，并立即卸钩，使弹窗看起来像真实的 Word 报错，以此迷惑用户、掩护后台恶意代码执行。

```

if ( v222 )
    qword_140054070 = (GetProcAddress)(v222, &v297);
CurrentProcess = GetCurrentProcess();
CurrentThread = GetCurrentThread();
v227 = GetCurrentProcess();
DuplicateHandle(v227, CurrentThread, CurrentProcess, &TargetHandle, 0, 0, 2u);
if ( qword_140054070 && TargetHandle )
{
    phNewTimer = nullptr;
    v228 = GetTickCount();
    CurrentProcessId = GetCurrentProcessId();
    CreateTimerQueueTimer(
        &phNewTimer,
        nullptr,
        Callback,
        nullptr,
        v228 % 0x88A + 8818,
        CurrentProcessId % 0x88A + 12734,
        0);
}
strcpy(v293, "crypt32.dll");
v230 = (LoadLibraryA)(v293);
if ( v230 )
{
    v297.m128i_i8[0] = 67;
    v231 = 1;
    v232 = &v297.m128i_i8[1];
    do
    {
        ++v232;
        v233 = byte_1400512F0[v231] ^ byte_140051400[v231 % 0xC];
        ++v231;
        *(v232 - 1) = v233;
    }
    while ( &v299 != v232 );
    v234 = (GetProcAddress)(v230, &v297);
    lpStartAddress = v213;
    if ( v234 )
        v234(0x10000, 0, 0, sub_140001610);
}
if ( hHandle )
{
    WaitForSingleObject(hHandle, 0xFFFFFFFF);
}
else
{
    Thread = CreateThread(nullptr, 0, v213, nullptr, 0, nullptr);
    if ( Thread )
        WaitForSingleObject(Thread, 0xFFFFFFFF);
}

```

图2 恶意代码执行沙箱在内存中检出 CobaltStrike 载荷，并成功提取其 C2 配置等关键信息，如图 3 所示。

家族	CobaltStrike
通信协议	HTTPS
C2 地址	https://nd-cohen.cn.cdn.dnsv1.com:443/sw.js
端口	443
URL	nd-cohen.cn.cdn.dnsv1.com/sw.js 111.6.166.81/sw.js 111.8.3.214/sw.js 112.46.50.58/sw.js 113.142.216.56/sw.js 116.153.4.140/sw.js 116.163.31.213/sw.js 116.163.31.218/sw.js 117.187.145.123/sw.js 119.0.110.63/sw.js 120.222.189.193/sw.js
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36

图3 威胁配置信息提取

样本二

- 样本名：张x-xx大学-个人简历.zip
- MD5：48da63173b01d21120c07d9b34227cb4
- 文件类型：zip
- C2：

43.144.20[.]241:4123119.91.242[.]155:1091

报告链接：[https://sandbox.qianxin.com/tq/report/toNewReport.do?](https://sandbox.qianxin.com/tq/report/toNewReport.do?rid=4bb0b7b1450d5db8a38ee25f5a41f5b1&index=1&sk=07155066)

[rid=4bb0b7b1450d5db8a38ee25f5a41f5b1&index=1&sk=07155066](https://sandbox.qianxin.com/tq/report/toNewReport.do?rid=4bb0b7b1450d5db8a38ee25f5a41f5b1&index=1&sk=07155066)

- 描述：该样本伪装成个人简历压缩包，运行后通过 Donutloader 加载执行 Shellcode，建立持久化后门；随后覆写关键系统函数绕过 ETW 和 AMSI 检测，最终连上 C2 服务器，等待攻击者下发指令。

Shellcode 加载：沙箱通过内存扫描检测到 Donutloader 加载器相关恶意代码，表明样本存在 Shellcode 加载行为，如图 4 所示：

内存 DUMP 检测

规则名	威胁类型	描述	危害	匹配	来源
R1_64_Hunting_Raw_ShellcodeEngine_StackStrings_R1Beta	Shellcode-ShellcodeEngine	-	信息	查看	TianQiong
Windows_Trojan_Donutloader_f40e3759	特洛伊木马-Donutloader	-	危险	查看	Elastic Security

图4 Shellcode 加载

ETW/AMSI 规避：样本尝试覆写 **EtwEventWrite**、**AmsiScanString** 等关键系统函数的代码，规避 **ETW (Windows 事件跟踪)** 日志监控和 **AMSI** 反恶意软件扫描，从而隐藏自身行为，降低被安全产品发现的可能性，如图 5 所示。

● 16:6:46.156	代码覆写	T1055 ×3	[3928] weixin.exe	疑似覆写 EtwEventWrite 函数代码段，试图规避 ETW 日志监控 成功(0)	危险 Process
● 16:6:46.156	代码覆写		[3928] weixin.exe	疑似覆写AmsiScanString模块代码块，规避应用层hook检查 成功 (0)	敏感 Process
● 16:6:46.156	代码覆写		[3928] weixin.exe	疑似覆写 EtwEventWrite 函数代码段，试图规避 ETW 日志监控 成功(0)	危险 Process

图5 代码覆写规避 ETW/AMSI

三、IOC 福利

HVV IOC

43.144.20[.]241:4123119.91.242[.]155:1091https://nd-cohen.cn.cdn.dnsv1[.]com/sw.jshttps://111.6.166[.]81/sw.jshttps://111.8.3[.]214/sw.jshttps://112.46.50[.]58/sw.jshttps://113.142.216[.]56/sw.jshttps://116.153.4[.]140/sw.jshttps://116.163.31[.]213/sw.jshttps://116.163.31[.]218/sw.jshttps://117.187.145[.]123/sw.jshttps://119.0.110[.]63/sw.jshttps://120.222.189[.]193/sw.jscloud-qd-ludrjwdidm[.]cn-qingdao[.]fcapp[.]runemp.icbcbc[.]com[.]cn/rewardsapp/ncfootererp.icbcbc[.]com[.]cn/analytics/v1_uploadapi.icbcbc[.]com[.]cngit.icbcbc[.]com[.]cnwebtest.icbcbc[.]com[.]cn163.181.35[.]238:443163.181.228[.]219:443117.126.128[.]9:443140.207.247[.]167:443111.124.194[.]162:443116.176.95[.]45:443101.227.5[.]171:443113.113.100[.]46:4431.194.31[.]501.82.232[.]57106.227.102[.]162111.124.194[.]166120.220.81[.]138122.228.214[.]50140.249.145[.]114171.43.169[.]135182.242.63[.]144183.60.202[.]51219.147.77[.]57220.181.166[.]11220.181.167[.]18027.152.185[.]1358.218.215[.]73uwitss[.]com111.230.218[.]210:42356https://82.156.5[.]140https://134.175.120[.]21968.64.183[.]64wocaoniba[.]org

文件

MD5	文件名
2b8975199cd350870fd6c7a4745f0f73	install_m3ue016.zip
b383f54492d3f16b446902aa720d0db8	install_s0sp005.msi
606f1310042c088ff67c9aa277d86ed0	2026.08.03裁员名单及补偿方案WPS.exe
2d4f738279d1874f4ef642c9ce57f8aa	install_n5w012.msi
f514e57bd3e66e36a25f91ccd2f99435	install_n5w013.msi
6064c2ac9a45b51ec8b3e86358800ff6	install_b6j007.msi
2bbfab27832794398d7a2a0199e964ad	install_b6j001.msi
3f70c3a5244cb2ca0b88f81b1b8df9bf	install_b6j019.msi
da6a114917bdb41286172fcaec6a05a3	新建文件夹.exe
9105fb31d2149633a1bb8670d6323873	LydiaPigou.zip
a2725962feab5c3424c7ffd1f0689912	2026.08.05裁员名单及补偿方案_sute.x64.exe
ab1d791117f08c8830dbb5436f341c05	setup_r8014_dowload.zip
7457acf4ae83faae52db909d15eab181	setup_r8010.exe
083316688a2a0e61f45c74a953053f55	wczt-win-8.1.65-x64 (1).exe
27a292bf49ef4daa90fd1bac78937d7c	一键设置中文语言.....exe
52bc38d7a1f167c876cca38099a7fb44	install_c0b016.exe
c5b2b23d907599a1de9dbf876640d2c4	install_c0b013.exe

域名/IP

https://unby6r.oss-cn-beijing.aliyuncs[.]com0nbay3.oss-cn-beijing.aliyuncs[.]com2026mn.oss-cn-hongkong.aliyuncs[.]com38.22.234[.]137:1082283newo.oss-cn-beijing.aliyuncs[.]combo2b8y.oss-cn-beijing.aliyuncs[.]comgxfsxs[.]cnhttp://aidrmvo[.]cning.yunshang[.]qponnanuvvo[.]cnupxrig[.]netxjsjkjdsjdd.s3.ap-southeast-1.amazonaws[.]com

天穹智能分析平台（联系我们申请账号）：<https://sandbox.qianxin.com>

天穹智能分析平台持续迭代升级，致力于为每一位样本分析人员打造更高效、更智能、更易用的分析平台——这始终是我们不变的初心与追求。

如果您希望深入了解平台功能，或在使用过程中遇到任何问题，欢迎随时联系我们。您的反馈，是我们进步的重要动力！