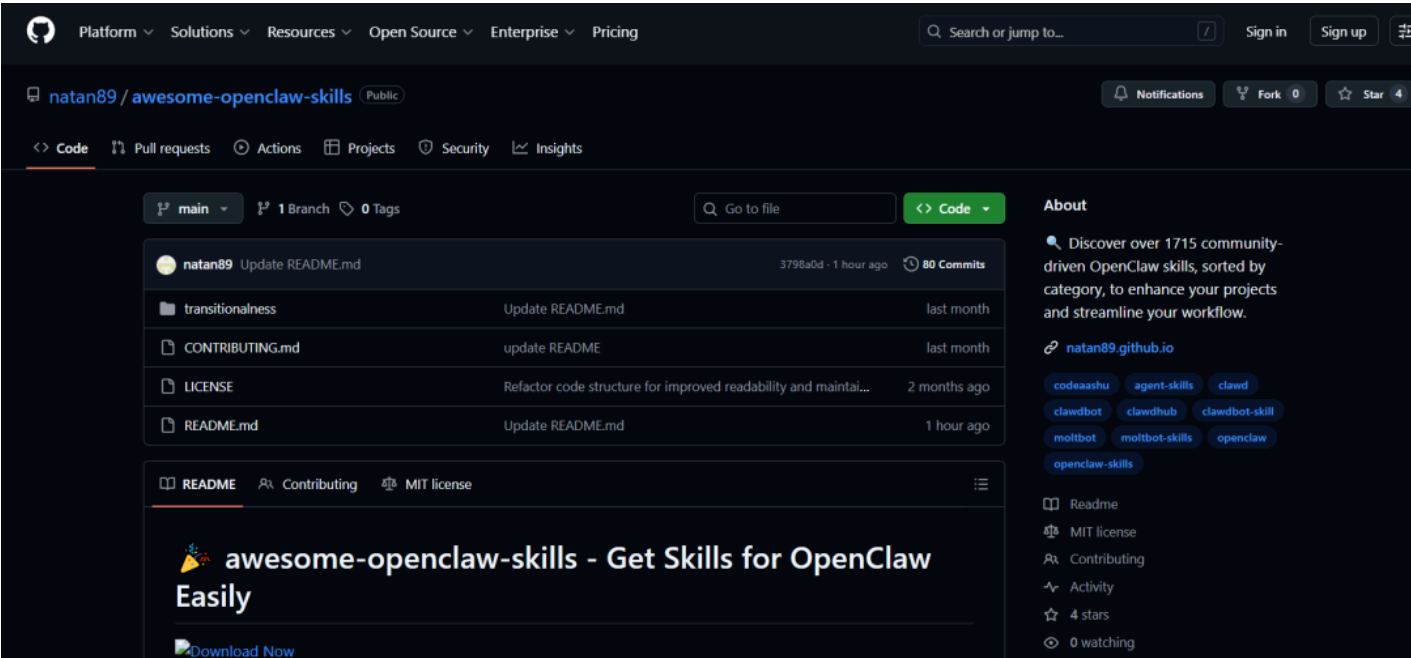


OpenClaw热潮之下，Lua窃密软件精心伪装乘虚而入

secrss.com/articles/88621



病毒木马 奇安信威胁情报中心 2026-03-19

攻击者通过 fork 高热度 Github 仓库实施伪装，使用的 Lua 窃密软件与 SmartLoader 恶意软件历史攻击活动的特征一致。

背景

前段时间兴起的 OpenClaw 热潮引发大量关注，不少人纷纷尝试安装体验。一些攻击者也嗅到了可乘之机，将恶意软件用 OpenClaw 相关话题进行伪装，诱使不明真相的用户运行使用，最终实现敏感数据窃取等目的。

奇安信威胁情报中心之前发布的文章：[《当心“龙虾”变“毒蝎”：你在GitHub上领的“龙虾”可能有毒！》](#)^[1]、[《OpenClaw管控困难？奇安信多款产品实现全维度闭环管控》](#)^[2]中提到多个利用 OpenClaw 话题的恶意软件攻击案例，本文是对第二篇文章中记录的通过 Github 传播的 Lua 窃密软件的进一步分析。我们发现攻击者通过 fork 高热度 Github 仓库实施伪装，使用的 Lua 窃密软件与 SmartLoader 恶意软件历史攻击活动的特征一致。

详细分析

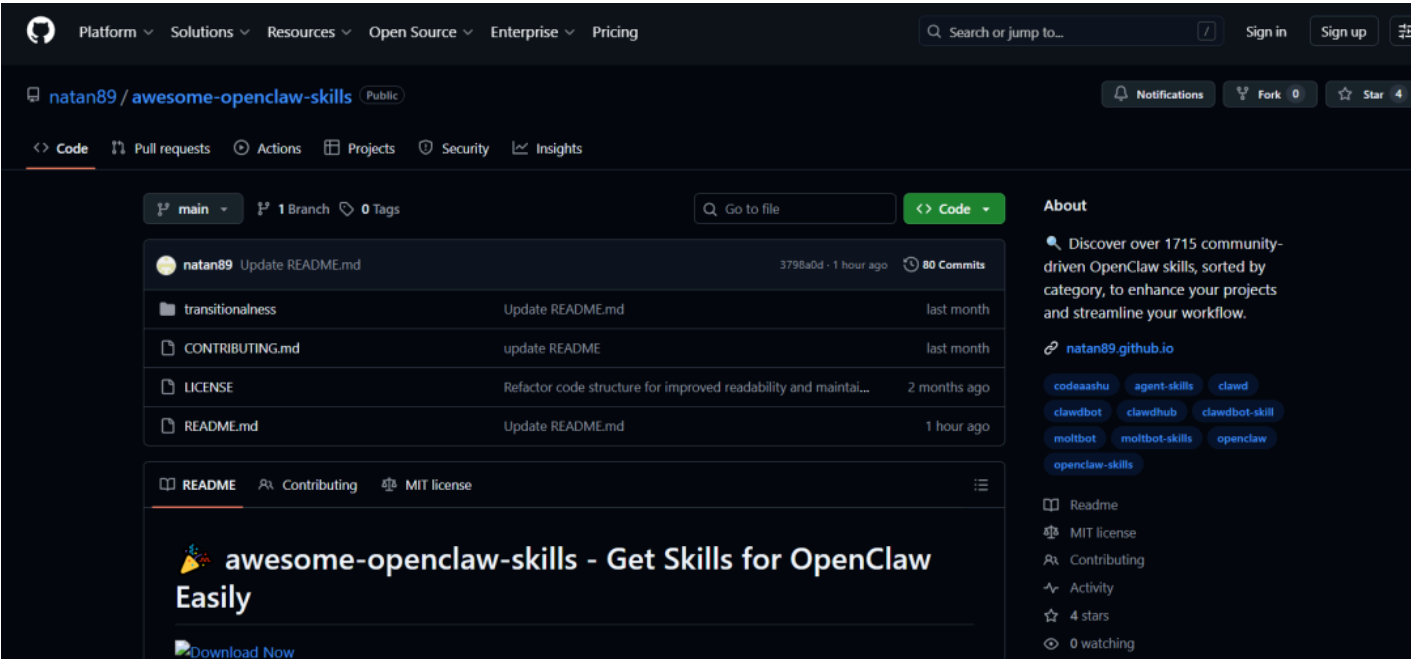
相关恶意样本信息如下：

MD5	文件名	Github下载链接
2023f00b8abc80b3b60fd556ab2a6672	openclaw-awesome-skills-1.6.zip	hxxps://raw.githubusercontent.com/natan89/awesome-openclaw-skills/main/transitionalness/openclaw-awesome-skills-1.6.zip
3cd87493759b8618782233153c5da73e	clawdbot_docker_2.9.zip	hxxps://raw.githubusercontent.com/challe09543211/clawdbot-docker/refs/heads/main/antimasque/clawdbot_docker_2.9.zip

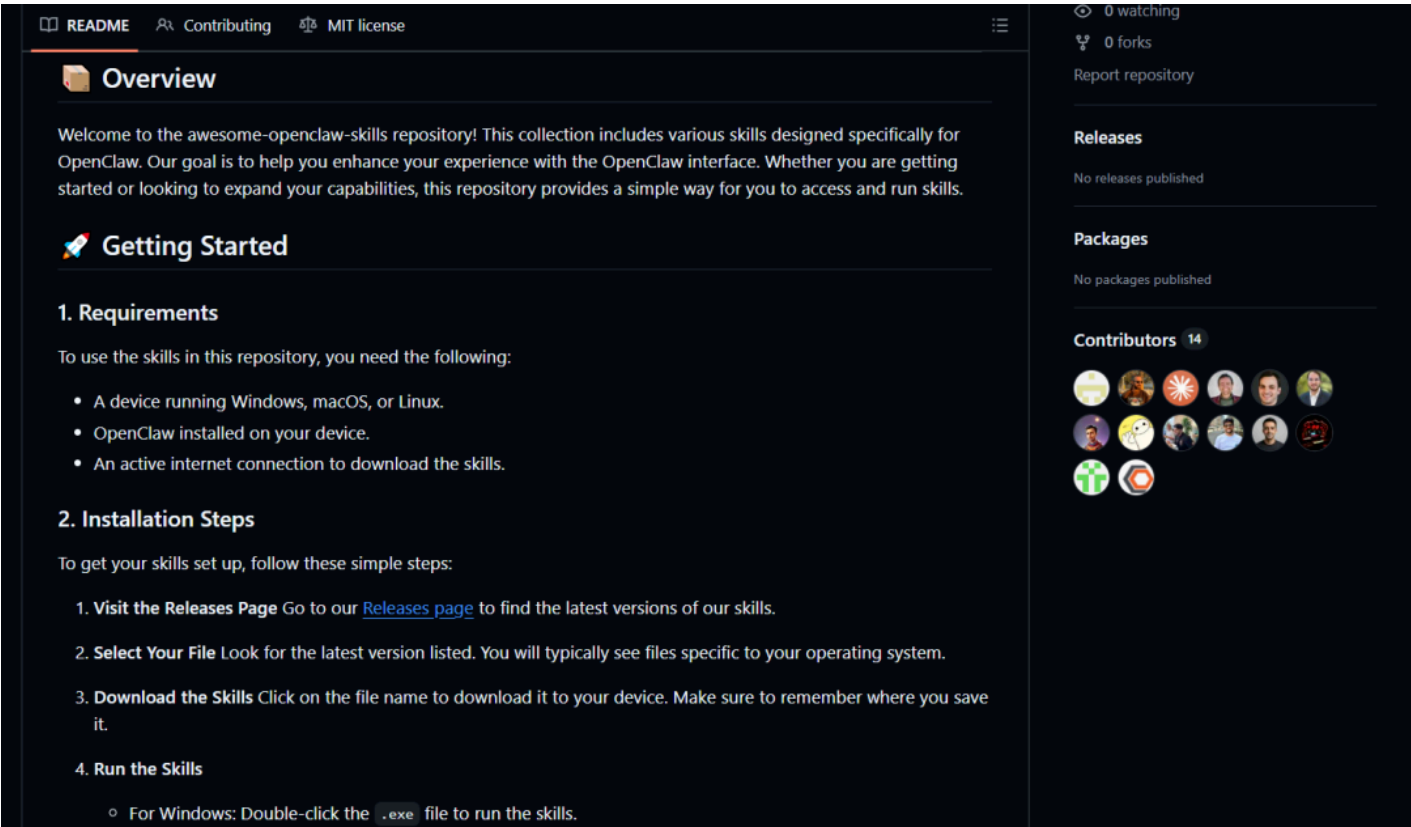
其中 clawdbot_docker_2.9.zip 对应的 Github 仓库 "challe09543211/clawdbot-docker" 目前已无法访问。

伪装的Github仓库

以 openclaw-awesome-skills-1.6.zip 为例，对应的 Github 仓库 "natan89/awesome-openclaw-skills" 伪装为 OpenClaw skills 的获取工具。



仓库通过多种方式增加可信度，比如看起来详细的 README.md 文档，有多个贡献者，有博客文章的介绍链接。



natan89

awesome-openclaw-skills - Unlock Amazing OpenClaw Features

[Download Now](#) [Click Here](#)

Description

Welcome to "awesome-openclaw-skills," the ultimate collection of OpenClaw Skills. This collection, formerly known as Moltbot, originally arose from Clawdbot. It provides users with various skills and functionalities designed to enhance your experience.

Whether you are looking to automate tasks or improve your projects, these skills can make your life easier. Our repository includes various features that cater to different needs, providing a robust set of tools to help you succeed.

Getting Started

To start using "awesome-openclaw-skills," follow the steps below. You will be up and running in no time.

1. System Requirements

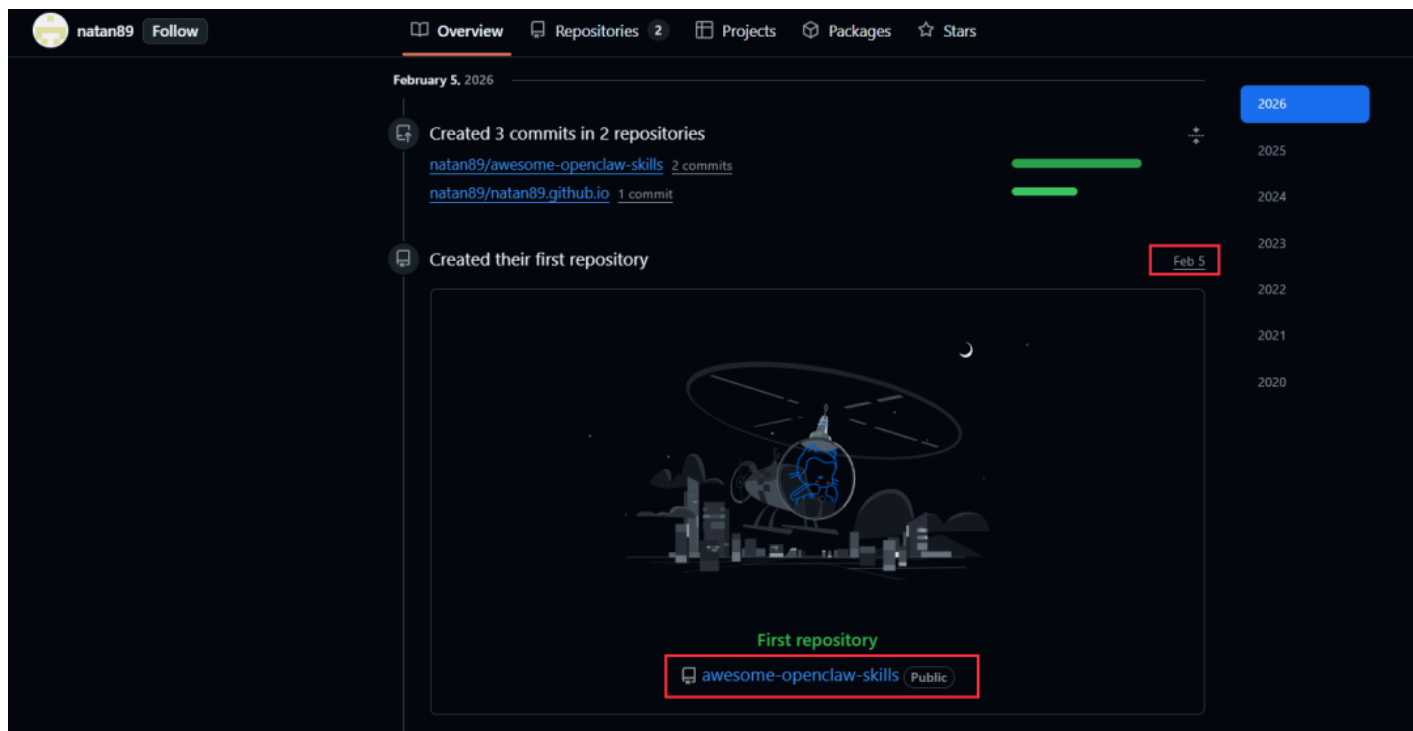
Before you download, please ensure your system meets the following requirements:

- Operating System: Windows 10 or later, macOS, or Linux
- Memory: At least 4 GB of RAM
- Disk Space: Minimum 200 MB available
- Internet Connection: Required for downloading and updates

我们认为最具有迷惑性的一点是：除了 natan89 这个用户，其他贡献者看起来都是正常账号。

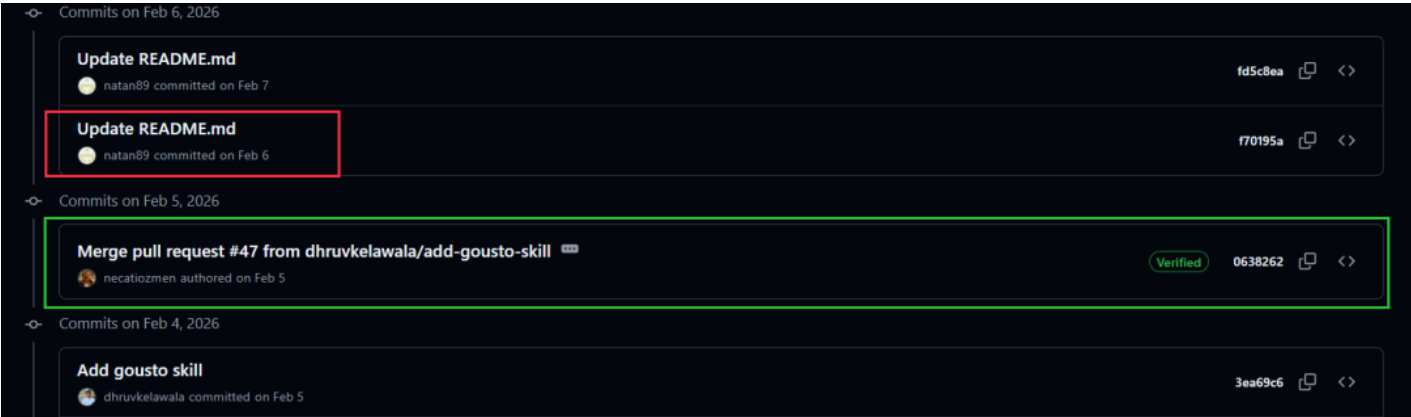
攻击者实现这一点的做法非常简单，他不是从零创建仓库，而是直接 fork 一个已知仓库，在上面提交自己的修改，增加恶意内容。

查看 natan89 用户的活动，在 2 月 5 日创建仓库 "natan89/awesome-openclaw-skills"。



The screenshot shows the GitHub profile of user natan89. The profile includes a header with the username, a 'Follow' button, and navigation tabs for Overview, Repositories (2), Projects, Packages, and Stars. The main content area displays activity for February 5, 2026. The first activity is 'Created 3 commits in 2 repositories', with links to 'natan89/awesome-openclaw-skills' (2 commits) and 'natan89/natan89.github.io' (1 commit). The second activity is 'Created their first repository', which is highlighted with a red box. Below this, a large image shows the repository 'awesome-openclaw-skills' with a 'Public' label, also highlighted with a red box. The right sidebar shows a calendar view for the year 2026, with the date 'Feb 5' highlighted in a red box.

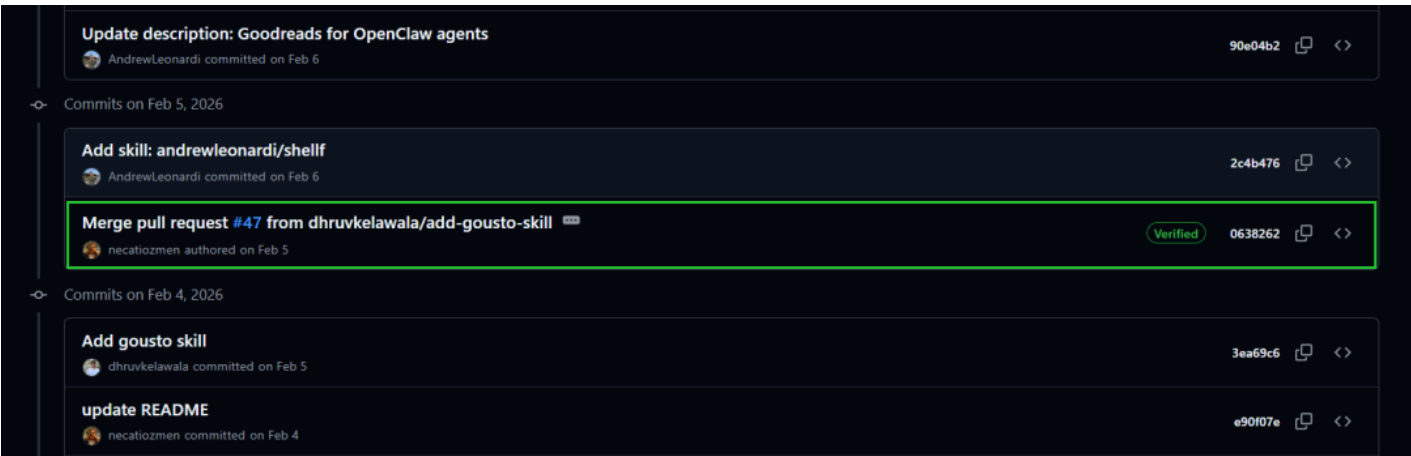
2月6日，natan89 用户提交 "natan89/awesome-openclaw-skills" 仓库的第一次 commit。上游 commit 由 necatiozmen 用户提交，commit 的 SHA-256 哈希为 0638262c744c292b4d67f01e8822d80686edfee0。



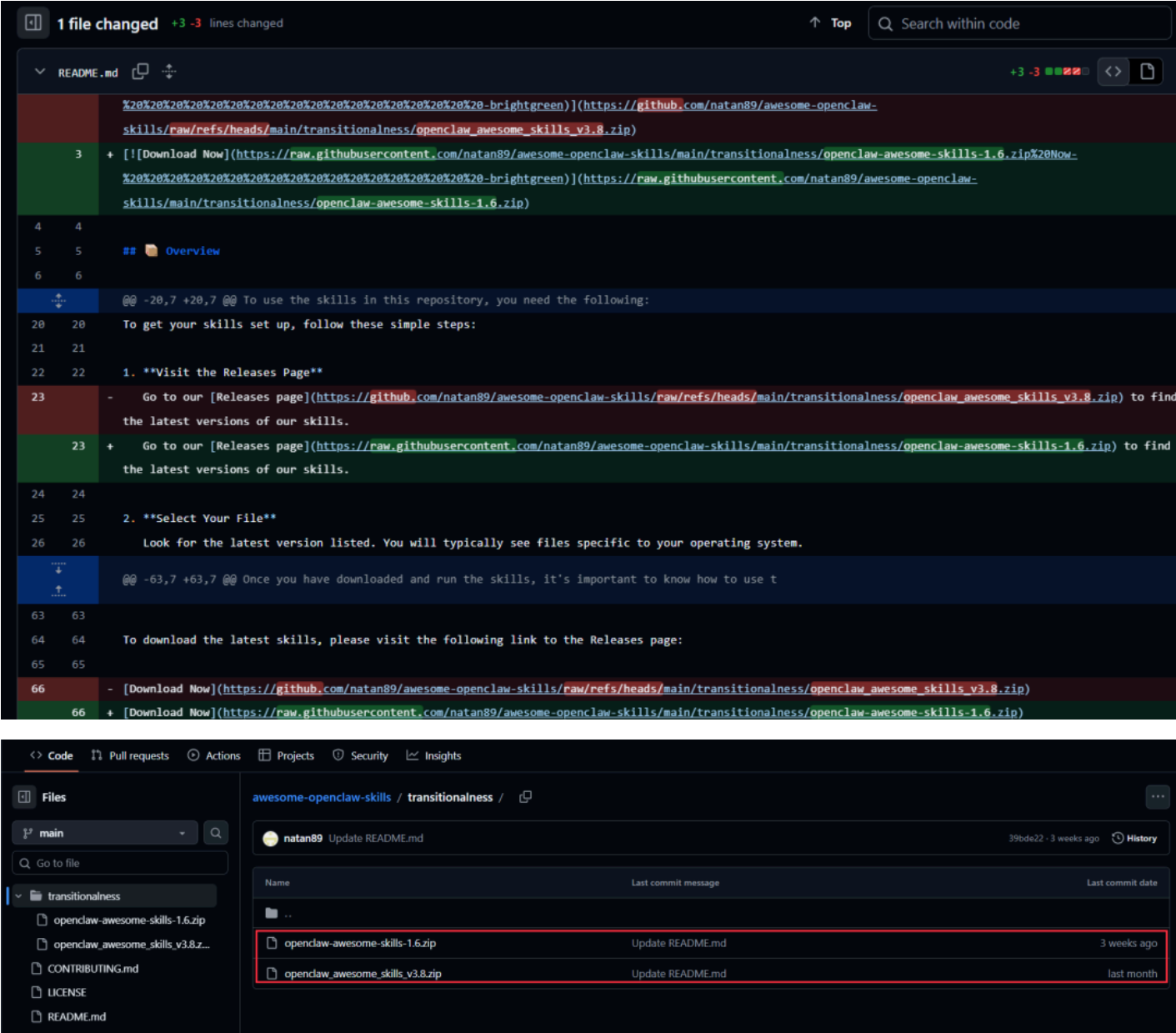
而 necatiozmen 用户本身管理一个同名仓库 "VoltAgent/awesome-openclaw-skills"，该仓库的 star 和 fork 数量均达到数千。



necatiozmen 在这个仓库 2月5日的一个 commit 的 SHA-256 哈希正是 0638262c744c292b4d67f01e8822d80686edfee0。说明攻击者是在此次 commit 之后对该仓库进行了 fork 操作。



恶意仓库 "natan89/awesome-openclaw-skills" 的 README.md 文件中出现的下载链接，指向这个仓库中托管的恶意ZIP文件。除了 openclaw-awesome-skills-1.6.zip，还有另一个恶意 ZIP 文件 openclaw_awesome_skills_v3.8.zip（MD5: badd55e31c9135845807bbb2ee2ff72b）。



Lua窃密软件

openclaw-awesome-skills-1.6.zip 中包含文件如下，Application.cmd 启动 compiler.exe，并以 dynasm.txt 为参数。

文件	大小	类型	日期	MD5
Application.cmd	29	Windows 命令脚本	2026/2/19 14:27	FE994EEA
compiler.exe	872,448	应用程序	2026/2/19 14:27	E6888E3E
dynasm.txt	308,347	文本文档	2026/2/19 14:27	33F25719

```
Application.cmd
1 start compiler.exe dynasm.txt
```

Compiler.exe 是 LuaJIT 程序，dynasm.txt 为经过混淆处理的 Lua 脚本。

Address	Length	Type	String
.rdata:00...	00000007	C	luaJIT
.rdata:00...	0000000F	C	%sinterrupted!
.rdata:00...	00000008	C	usage:
.rdata:00...	000001E0	C	[options]... [script [args]...] \n\nAvailable options are:\n -e chunk Execute string 'ch
.rdata:00...	0000001F	C	(error object is not a string)
.rdata:00...	00000008	C	__tostring
.rdata:00...	0000004D	C	LuaJIT 2.1.0-beta3 -- Copyright (C) 2005-2017 Mike Pall. http://luaJIT.org/\n
.rdata:00...	00000008	C	_LOADED
.rdata:00...	00000007	C	status
.rdata:00...	00000008	C	JIT: ON
.rdata:00...	00000009	C	JIT: OFF
.rdata:00...	00000008	C	require
.rdata:00...	00000008	C	_PROMPT
.rdata:00...	00000009	C	_PROMPT2
.rdata:00...	00000008	C	'<eof>'
.rdata:00...	0000000A	C	return %s
.rdata:00...	00000007	C	=stdin
.rdata:00...	00000006	C	print
.rdata:00...	0000001B	C	error calling 'print' (%s)
.rdata:00...	00000008	C	module
.rdata:00...	00000006	C	start
.rdata:00...	00000036	C	unknown luaJIT command or jit.* modules not installed
.rdata:00...	00000008	C	jit.opt
.rdata:00...	00000007	C	bcsave
.rdata:00...	00000010	C	=(command line)
.rdata:00...	00000009	C	LUA_INIT
.rdata:00...	0000000A	C	=LUA_INIT
.rdata:00...	0000000A	C	LUA_NOENV
.rdata:00...	00000027	C	cannot create state: not enough memory

```

return(function(...)local x=function(u)local x=""for k=1,#u/2,1 do x=x..u[#u/2+u[k]]end return x end return(function(u,I,h,T,L,O,y,k,H,Y,E,C,
C,w,Z,W,K,z,J,m,V,B,q)J,k,z,C,K,Z,B,q,E,w,V,Y,m,W,H,c=function(u,x)local I=H(x)local h=function(h,T,L,O,y)return k(u,{h;T,L,O,y},x,I)end
return h end,function(x,k,h,T)local vH=function(u)local x,k=u[#u],""for I=1,#x,1 do k=k..x[u[I]]end return k end local GH=function(u)local
x=""for k=1,#u/2,1 do x=x..u[#u/2+u[k]]end return x end local AH,eH,Q,L,zH,jH,F,j,CH,N,hH,tH,mH,rH,s,MH,M,X,W,QH,iH,IH,nH,p,BH,A,P,LH,a,VH,SH,
HH,xH,UH,d,fH,ZH,kH,e,b,S,uH,NH,l,yH,OH,aH,dH,f,E,RH,g,C,r,V,gH,R,G,U,H,o,VH,sH,lH,TH,EH,qH,v,y,DH,JH,i,CH,wH,D,t,FH,pH,n,KH while x do if
x<8090859-(-235501)then if x<1010222+3467716 then if x<1524575-(-1610402-(-889400))then if x<-93674+1246781 then if x<239896+476506 then if
x<900967+-605920 then if x<((-110050+-872659)+438364)-(-733058)then if x<133306+-63084 then if x<-807932+869712 then if x<-431237+485334 then

```

Lua 脚本运行后调用 CreateMutexW 函数，创建互斥量。



将收集的信息加密后和截屏数据发送到 "hxxp://89.169.12.235/api/NTE3YjdjNWU1NjYzNjU2YTA1N2Y="。

openclaw_awesome_skills_v3.8.zip 中的 Lua 恶意脚本执行流程类似，回传数据的 URL 为 "hxxp://213.176.73.145/api/NTE3YjdjNWU1NjYzNjU2YTA1N2Y="。

clawdbot_docker_2.9.zip 中 Lua 脚本回传数据的 URL 为 "hxxp://213.176.73.162/api/NTE3YjdjNWU1NjYzNjU2YTA1N2Y="

溯源关联

89.169.12.235，213.176.73.145，213.176.73.162 这三个 IP 在 VirusTotal 平台上关联了多个类似的仿冒各种工具的恶意 ZIP 样本。

此次发现的利用 OpenClaw 相关话题的恶意软件攻击流程和特征与多篇公开报告^[3~5]中描述的 SmartLoader 恶意软件攻击行动一致。

(1) 均使用经过混淆处理的 Lua 脚本，通过 ip-api[.]com 获取公网IP信息，访问 www.microsoft[.]com 测试网络联通性，获取 MachinGuid、主机名、用户名等信息。

(2) 收集的信息向 C2 服务器的 "/api/" 路径发送，并且还会携带截屏数据。

这种借用虚假 Github 仓库传播的 Lua 窃密软件至少在 2024 年就已经出现，并且一直处于活跃状态。根据开源报告，该恶意软件具备部署其他恶意载荷的能力，可以用于植入 Lumma Stealer 等功能更加完备的窃密软件。

总结

OpenClaw 的火热让多个恶意软件攻击团伙找到了具有高传播度的诱饵话题，以此对恶意软件进行重新包装，增加恶意软件被安装的机会。在此次攻击活动中，攻击者借用 fork 合法 Github 仓库的方式，复用了仓库 commit 活动历史以及贡献人员，巧妙地提升了伪装仓库的可信度，然后在此基础上再添加恶意内容。如果用户不加分辨地使用来自这种开源仓库的程序，将面临恶意软件感染、敏感数据遭盗取等潜在风险。

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

(ZIP)

2023f00b8abc80b3b60fd556ab2a6672

3cd87493759b8618782233153c5da73e

badd55e31c9135845807bbb2ee2ff72b

(恶意Lua脚本)

e482d9f2f0cdcd1b388e10c105f66502

04030b8bc36740bdd81744faaba58d3

888422ff5b733231eb715ce97eefaaf0

C&C

hxxp://89.169.12.235/api/

hxxp://213.176.73.145/api/

hxxp://213.176.73.162/api/

参考链接

[1].https://mp.weixin.qq.com/s/jNYCA9G1jSkevgPWv4Ov_Q

[2].<https://mp.weixin.qq.com/s/LISl5pdIBDJ53d9ZbdOq4w>

[3].<https://www.morphisec.com/blog/threat-analysis-lua-malware/>

[4].<https://www.trendmicro.com/en/research/25/c/ai-assisted-fake-github-repositories.html>

[5].<https://blog.intellibron.io/lua-jit-smartloader-analyzing-the-github-campaign-delivering-stealer/>

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

- [**“网络洲际导弹”泄露！数亿台iPhone可被静默入侵窃取所有数据**](#)

[病毒木马](#) [安全内参](#) 2026-03-19

[谷歌等多家安全公司披露，近期在公网上发现DarkSword、Coruna等多个iPhone入侵工具的攻击行为，已被俄罗斯等多个威胁组织和间谍软件肆意使用，用于在水坑站点窃取针对性目...](#)

- [**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假冒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...](#)

- [**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。](#)