KELA

Chinese cybercrime ecosystem

All that you need to know about
Chinese cybercriminals in 2024

Table of contents

Please note this is a redacted version of the report where the specific names of Chinese cybercrime platforms have been anonymized in order to protect the confidentiality and integrity of ongoing investigations and to prevent potential harm. Throughout the report, pseudonyms such as "Market1" and "Channel1" have been used to reference these sources. If further clarification or access to the actual names of the platforms is required, please contact KELA’s marketing team for assistance: marketing@ke-la.com.

Executive summary

In 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) shifted its focus to Chinese-linked cyber threats, considering the People's Republic of China to be the top nation-state threat, along with Russia, North Korea, and Iran.[1] In relation to this, researchers note that the amount of cyber attacks by Chinese state-sponsored groups and their severity have increased in recent years.[2]

In parallel, the number of cybercrime cases, based on data from China's criminal courts, has also been increasing.[3] Most recently, Chinese-language malware spread via email campaigns has also witnessed a rise, another indicator of an uptick in cybercrime activity originating from China.[4]

This mutual growth of financially motivated Chinese cybercriminals and state-sponsored advanced persistent threats (APTs) is related to the fact that both are integral parts of the same cybercrime ecosystem. The blurred line between state-sponsored actors (usually aiming for espionage) and financially motivated actors in China allows for shared resources and expertise to flow between the two groups. State-sponsored APTs often use a vast pool of technical talent and sophisticated tools, some of which may find their way into the hands of financially motivated cybercriminals. In a similar way, these APTs can leverage tools created and distributed among financially motivated actors.

Following the growing Chinese cyber threat, KELA has researched the Chinese-speaking cybercrime ecosystem to empower enterprise defenders to make informed decisions and fortify their cyber defenses against the challenges posed by these threats.

This report will cover:

- **Background:** The historical context and the impact of government actions on the cybercrime landscape, as well as cultural perspectives on "dark" and "gray" crime, shaping the perception and dynamics of cybercrime activities in China.
- **Chinese-speaking cybercrime platforms 2024:** An overview of current platforms, categorizing them into tech-oriented forums and cybercrime markets, as well as analysis of the Telegram fraud ecosystem, highlighting hacking-as-a-service, the trade in credit-card data and counterfeit IDs, money laundering, and bypass services.

[1] CISA pivots focus to China-linked threats against critical infrastructure; People's Republic of China Cyber Threat

[2] Criticality of Chinese cyber threat actors has increased in recent years

[3] China's cyber crime problem is growing; 司法大数据专题报告显示——涉信息网络犯罪案件量逐年上升，诈骗罪占比最高

[4] Report: Increase in Chinese-Language Malware Could 'Challenge' Russian Dominance of Cybercrime

- **The presence of Chinese-speaking actors on non-Chinese cybercrime platforms:** The integration of financially motivated actors as well as the connection between Chinese APTs and cybercrime sources.

In the context of this report, the term "Chinese cybercrime ecosystem" refers to the Chinese-speaking area of the cybercrime ecosystem, where individuals engaging in cybercrime and threat activities are creating interdependent relationships with their own rules and mechanisms. Accordingly, "Chinese cybercriminals" refers to Chinese-speaking threat actors active across different platforms and engaging in malicious activities.

Background

The influence of government action

China has been tightening controls over the country's information and the global cyberspace over the past years, which has influenced the cybercrime ecosystem as well.

In addition to enacting legislation in 2017 aimed at limiting cybercrime, including content regulations, China has rules that limit people's ability to use the Internet anonymously. The rules formulated what some researchers refer to as an "Internet real-name system" in China. For example, the rules mandate that service providers require users to provide real identities to use the Internet, chat groups, online forums, and social media, with partial penalties for the operators on violation.[5] This means users can use handle names for forums or social media, but their IDs should be stored and can be accessed by the authorities when necessary. Although some criticism, particularly from a Western perspective, characterizes this as a human-rights violation, it has dealt an effective blow to China's domestic sources of cybercrime.

The legal advancements in China have fostered a climate of self-censorship among major and minor website operators as well as users of hacking forums and blogs in the country, discouraging open activity by cybercriminals on the platforms. Such websites saw a trend toward the suppression, avoidance, and deletion of discussions that might be – or might be perceived as being – associated with criminal activities.[6]

The government has also conducted a series of successful crackdowns on cybercrime and fraud operations. Some of the well-known crackdowns include those on China Empire (in Chinese: 华中帝国), Hack80, White Ant (白蚁网安), and Red-Blue Security Net (红蓝安全网) in 2018 and TeaHorse (茶马古道) in 2022.[7] Furthermore, the steps that the authorities have taken against the use of VPNs and cryptocurrency may have significantly reduced the thriving cybercrime market operations and participation from China. Researchers also point out that in recent years an increasing number of Chinese cybercrime gangs have been moving their operational base abroad, using cryptocurrencies to launder money.[8]

Based on the cybercriminals' chatter, KELA finds that some of them overtly show off that they are based outside of China or that they travel back and forth between China and their bases elsewhere. Based on KELA's analysis, these actors are most commonly involved in financially motivated cybercrime, particularly credit-card fraud and theft of databases for sales

[5] Shrinking Anonymity in Chinese Cyberspace

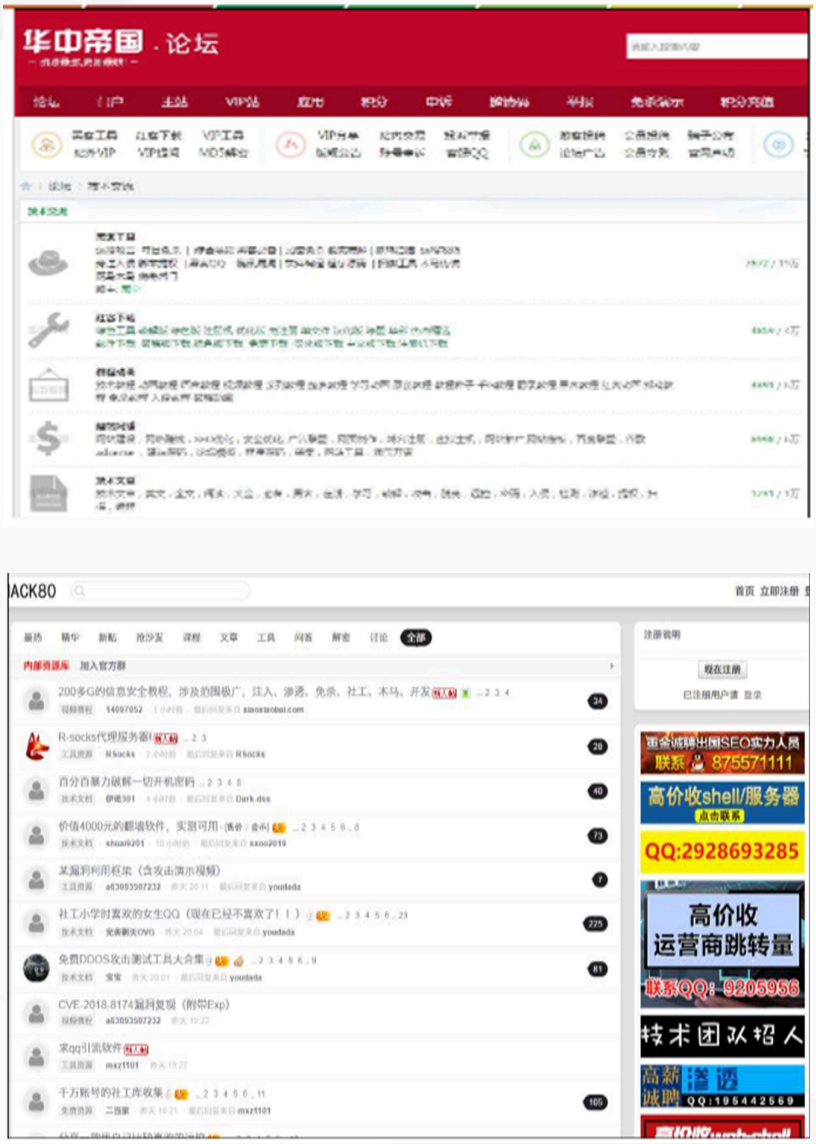
[6] Example websites: 52pojie, ihonker, CN-sec

[7] https://www.anwangxia.com/1555.html

[8] How Chinese Cybercriminals Use Business Playbook to Revamp Underground

purposes, though some of them are also engaged in organized and wide-ranging criminal activities that are not limited to cybercrime.

By 2024, based on KELA's monitoring, the count of active and individual Chinese-based cybercrime platforms with explicit exchange of criminal activities had narrowed down to a few.



Hack80 and CentralChineseEmpire (华中帝国), Chinese-speaking hacking forums that were closed down and the operations prosecuted by law enforcement in 2018. Source: t00ls

Local concepts of "dark" and "gray" crime

When speaking about the Chinese-speaking cybercrime landscape, it's important to understand two concepts derived from criminal terms that preceded the cyber era:

Hei-industry (dark industry) encompasses clearly illegal activities. In the context of cyber activities, these may include targeted and sophisticated cyber attacks that involve the theft of sensitive data, data corruption, denial of service, and so on. The term "hei" echoes the Chinese translation of the word "hacker," emphasizing the malicious and destructive nature of these activities. In a non-cyber context, it includes crimes such as murder and kidnapping.

Hui-industry (gray industry) involves unequivocally illicit but less prosecutable activities, particularly financial fraud. However, the unique legal context in China, marked by strict laws and sporadic prosecutions, may contribute to the perceived autonomy of gray industries from more overt criminal activities. In a non-cyber context, such gray industries could be related to financial fraud and unlicensed business.

With the Chinese government's rigid law enforcement and prosecutions over cybercrime, the Chinese-speaking ecosystem of the hackers in the "hei-industry" (a dark one) may be dying down. The remaining dark hackers seem to have intersected with the "gray industries," especially on the Telegram messaging platform. Therefore, most of the activities that are observed in the Chinese-speaking cybercrime ecosystem are related to financial fraud or other activities targeting individuals in a non-sophisticated manner. As for sophisticated cybercrime, explicit exchanges pertaining to advanced cyber threats are less likely to be spotted openly.

Chinese-speaking cybercrime platforms 2024

The current Chinese-speaking cybercrime ecosystem can be divided into 3 levels:

On the **"surface"** level, there are tech- and infosec-oriented **hacking forums** that don't explicitly offer malicious services. However, the content implies they may be used by cybercriminals.

On a **deeper** level are two of the most popular and stable Chinese-language cybercrime platforms: **Market1** and **Market2**.

Instead of traditional platforms (web-based markets, forums, etc.), the **Telegram instant messaging application** has become an integral part of the cybercrime ecosystem. As KELA noted in the report *Telegram: How a messenger turned into a cybercrime ecosystem by 2023*, this platform has become of great importance among cybercriminals, and this is also the case with the Chinese-speaking threat actors.[9] Given the tightened restrictions on anonymous use of the Internet, it's natural that the Chinese-speaking actors are increasingly using foreign apps instead of Chinese apps.

Tech- and infosec-oriented hacking forums

There are multiple Chinese-speaking hacking websites, such as t00ls, Kafan, and 52pojie, that openly publish and discuss hacking tools and exploit codes, which any member can obtain. However, most of these websites now explicitly exclude any illegality and display disclaimers such as "illegal activity is prohibited" and "use of software, samples, tools, etc., is for research and investigation purposes only."

Some forums publicly state that they self-censor and ban accounts that mention illegal activities as "offenders" in a section often called "little dark room" (小黑屋). This pronounced trend toward exclusion of illegality may be due to the increased severity of the censorship: KELA observed that some hacking community websites were shut down or depopulated between 2017 and 2018[10] if not rebranded as a law-abiding info security community.[11]

[9] Telegram: How a messenger turned into a cybercrime ecosystem by 2023

[10] Examples include forums such as华盟网 and Hack80

[11] Examples include forums such as 红黑联盟

To register to such websites, users must disclose their real identity, such as resident ID number and phone number, to the operator.

Many of the shared hacking tools are directly sourced or referenced from GitHub, and some are linked to famous underground websites. Additionally, one of the common methods for sharing items on such hacking forums is to refer to separate Chinese storage or resource-sharing platforms that are used to store malicious samples. Many such platforms offer users miscellaneous and harmless content mixed with some hacking tools.

Cybercrime markets

Market1

Launched in 2013, Market1 is one of the most well-established Chinese underground forums.

The marketplace has the following nine categories:

- Database and information (数据与信息)
- General services and operations (常规服务与操作)
- Physically delivered goods (实体发货商品)
- Technical services [non-tutorial] (技术服务[非教程])
- Film and TV sources (影视猎奇资源)
- Virtual items (虚拟物品)
- Tutorials and materials (教程与文档)
- Private auctions (私人专拍)
- Other (其它类别)

Per KELA's review, leaked or stolen databases and tutorials on hacking operations are the most frequently offered items on Market1.

The landing page of Market1. The first three categories of the market are displayed on the top: databases and information, general services and operations, and physically delivered goods.

A Market1 offering of user data from a UK retail brand, allegedly of 500,000 lines, including names, IP addresses, and phone numbers.

The format of the market is simple: Sellers (商家) post offerings with descriptions, samples, and prices in USD. The forum takes membership fees and charges a commission per transaction. Creating an account on Market1 is easy and doesn't even require an email address. However, to post items and comments, the account has to be upgraded to a "merchant account" by adding a referer or paying a subscription fee. The subscription fee is either 0.00007 BTC (approximately USD 3) for three months or 0.00028 BTC (USD 12) for a year. Per KELA's review, these are relatively low fees for cybercrime platforms.

Indeed, Market1's price page compares itself to "non-underground markets such as Amazon, which requires a high price to become a seller" and adds that "unlike Amazon that takes 10 days to pay the transaction value, our business will pay the seller immediately when the transaction is closed."

网站首页 -- 商家权限

洋葱路由保护您的私人隐私不被泄露, 本站网页代码不含Javascript, 您的所有信息都是私密的.
成为本站的商家, 您将得到更多的商业机会以及畅所欲言的探讨合作.

ID	类别	期限	费用[比特币]	操作	
1	商家权限	3个月	0.00007	支付费用	发布交易必须具备商家权限
2	商家权限	12个月	0.00028	支付费用	

*. 低门槛的商家认证资格是你事业起步的垫脚石.
对比亚马逊等诸多表网交易市场需缴纳数万美金质押才能成为商家, 占用周转资金, 本站商家认证门槛低, 起步很容易.
相对于亚马逊等在线商店的商家, 商品售出后1-2个月才能得到回款, 本站回款时间快, 买家确认收货后约10天左右就能回款, 资金急速回笼.

*. 请遵守交易市场公共规则.
作为商家, 请以身作则遵守交易诚信机制, 规避不必要的站外联系. 当你发出站外联系意向时, 您同时在诱导对方泄露隐私.

*. 请勿注册多个账户进行进行商家业务.
马甲账户没有任何意义, 本站有重新编译执行洋葱路由, 即便你换账户, 洋葱路由发来的信号是相同的.(对抗网络攻击的措施).
同时, 网站诚信机制更新后, 在线时间, 主动解答问题次数都作为加分项, 老商家更容易培养诚信.

*. 请重视对买家的服务承诺
当前本站对商家的认证资格非常低, 如果发生大量的怠慢买家的情况, 本站会提高商家资格.

Market1's membership subscription menu and disclaimers. One of the disclaimers claims, "Our qualification for users to become a merchant is very easy. If too many non-rule-abiding merchants arise, we may reconsider the qualification in the future."

As for the general pricing of the items for sale, some typical offers included corporate databases offered for USD 200–500, DDoS-as-a-service offered for USD 50 per attack, and a phishing tutorial package offered for USD 100.

Buyers can comment on the post and move on to direct messages or transactions. Transactions are done through BTC via Market1, not using the private wallets of sellers.

An actor offers to steal a database from a specific company per a buyer's request, with the price tag of USD 200. However, the seller clarifies that the exact price will be quoted after receiving a target domain or application.

Per KELA's review, there seems to be no strict peer-review mechanism to maintain the general quality of the items sold on Market1. For example, KELA has observed multiple cases where duplicate items are offered for sale by the same user under different descriptions. KELA also has observed cases where databases with a false description of the source remain on the platform without attracting critical comments, such as a publicly available database offered for sale for a high price with a false description that the data originated from a government breach.[12] Such falsified sales claims would have been flagged by users and removed by moderators immediately on the major English-speaking forums, such as BreachForums, for example.

Additionally, Market1 users can't view other users' profiles or search items by sellers. Each username is represented by a simple seven-digit unique number, and one user's activity can't be tracked by other users on the platform. Such mechanisms may be designed to provide anonymity to users, but they may not increase the market's credibility or reduce transaction frauds between users.

[12] Detected by KELA's research.

In 2023, the operators of Market1 implemented a scoring system for sellers and buyers. Items are tagged by sellers' reputation score, activity numbers, popularity, and hours online, information that purportedly is available only to the market admins. The users' reputation score may be accumulated scores given between users upon transaction. According to Market1's description, this system is meant for buyers and sellers to prioritize users with higher scores for making deals.

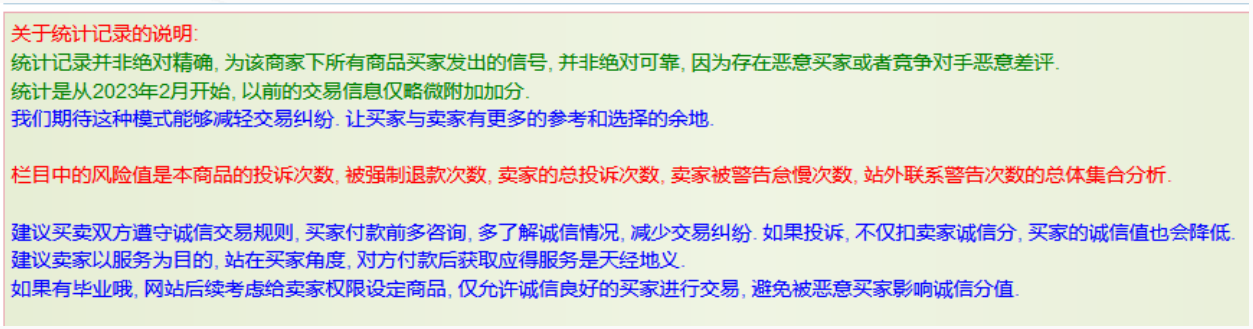
账户中心 充值 提币 资金记录 交易记录 我的发布 我的收藏 使用说明 其它 返回首页

网站首页 常规服务与操作

排序: 发布时间 更新时间 [记录不精确, 只从2023-2开始统计, 更多说明在下方] 1 2 3 4 5 9

ID	卖家	商品标题	美元标价	BTC成交额	成交量	好评:风险	咨询	热度	卖家在线	操作
1	1891833	人车公司信息在线查询	3			1534 : 0	43	30554	9小时	打开
2	715692	———渗透测试———网站脱裤———	200	0.0359	25	4476 : 21	778	86026	134小时	打开
3	680411	—侦探业务查询—全网高质量最低价—卖家Unicorn	1.4	5.3497	230264	15336 : 37	10823	131983	272小时	打开
4	639133	老线回归个人户籍车辆档案查询24h在线	3	0.7897	20914	10110 : 102	4857	169492	91小时	打开
5	752509	柯南侦探社查询就是快	1.6		3933	1795 : 4	775	31561	135小时	打开
6	25414	重开 如何解决你遇见的那些讨厌的人	3000	0.2363	8	1989 : 42	598	36938	23小时	打开
7	759062	打包—批盗u秒u提币等源码	55			23 : 2		162	47小时	打开
8	494256	做微信—手号商自己注册自己卖	25	0.1055	84	3464 : 63	205	67898	59小时	打开
9	715692	———网站渗透———测试评估———	200	0.0024	7	3176 : 18	238	61610	134小时	打开
10	533761	打手黑帮服务	15	0.6239	1416	3346 : 38	1871	60472	98小时	打开
11	591243	国内外撞库服务	1		1	286 : 32	9	4002	132小时	打开
12	639133	信誉商家老字号个人信息查询全天在线	20		230	902 : 60	192	10440	91小时	打开
13	1889980	VN_越南_Zalo_Business扫脸实名成品号VPN	2		2	1122 : 0	11	22212	38小时	打开
14	636430	各网站平台手机app各行业数据抓取为电销短信提供	15	0.0798	212	3976 : 36	2059	67305	52小时	打开
15	628526	匿名电报机器人搭建隐藏真实IP防止网警追踪做黑产	50	0.0084	7	4189 : 47	93	82512	166小时	打开
16	1884393	足球体育竞彩吸粉主动加你微信	50		4	1998 : 9	30	39486	20小时	打开
17	721799	———域名——劫持——跳转———	200			656 : 15	4	12252	77小时	打开
18	715692	——DDOS攻击——任何的——有效的——	50			343 : 16	15	5475	134小时	打开

Each offering can be sorted by price, users' historical transaction volume, "reputation:risk," search amount, reputation score, and hours spent on the platform.



关于统计记录的说明:
统计记录并非绝对精确, 为该商家下所有商品买家发出的信号, 并非绝对可靠, 因为存在恶意买家或者竞争对手恶意差评.
统计是从2023年2月开始, 以前的交易信息仅略微附加加分.
我们期待这种模式能够减轻交易纠纷. 让买家与卖家有更多的参考和选择的余地.

栏目中的风险值是本商品的投诉次数, 被强制退款次数, 卖家的总投诉次数, 卖家被警告怠慢次数, 站外联系警告次数的总体集合分析.

建议买卖双方遵守诚信交易规则, 买家付款前多咨询, 多了解诚信情况, 减少交易纠纷. 如果投诉, 不仅扣卖家诚信分, 买家的诚信值也会降低.
建议卖家以服务为目的, 站在买家角度, 对方付款后获取应得服务是天经地义.
如果有毕业哦, 网站后续考虑给卖家权限设定商品, 仅允许诚信良好的买家进行交易, 避免被恶意买家影响诚信分值.

According to a disclaimer on the website, such scoring is based on its data starting from February 2023.

Per KELA's data, from 2018 to 2021, the number of posts on Market1 remained constant at 4,000 to 5,000 per year, but the volume of posts significantly decreased by about half in the period around 2022. Additionally, in 2023, the website suffered multiple issues that may have damaged its reputation. In April 2023, users accused Market1 of confiscating Bitcoins from multiple users by freezing their accounts without legitimate reasons, leading to one user

claiming to have hacked Market1 to prove it.[13] Users also criticized Market1 for its extremely high commission rates.

However, Market1 has not been silently dying down. In September 2023, it announced that it had lowered commissions per transaction from nearly 50% to approximately 8%, possibly aiming to increase user numbers and activities.[14] While the recent changes related to reputation score may have helped Market1 gain trust from its underground users, the large number of newcomers may be further degrading the overall credibility of the deals and discussions on the platform, possibly damaging Market1's reputation.

Market2

Market2 (长安不夜城) emerged as a new Chinese underground market in its current form in September 2022.

The market's nine categories are similar to those of Market1:

- Data resources (数据资源)
- Film, TV, audio, and video(影视音像)
- Technical skills(技术技能)
- Card material, CVV(卡料CVV)
- Physical items(实体物品)
- Services(服务业务)
- Private auctions(私人专拍)
- Virtual items(虚拟物品)
- Other(其他类别)

Per KELA's review, the most active sections relevant to cybercrime are "Data resources" and "Card material, CVV," where leaked databases, stolen credit-card data, and personal information – including pictures of IDs (fake and stolen) – are offered for sale. The "Technical skills," "Services," and "Other" sections are very active, too. Among popular items are VPN software and tutorials associated with the use of VPN and other anonymity techniques; hacking tools, such as ransomware and malware; and hacking-as-a-service, such as gaining access to a victim's network and obtaining databases.

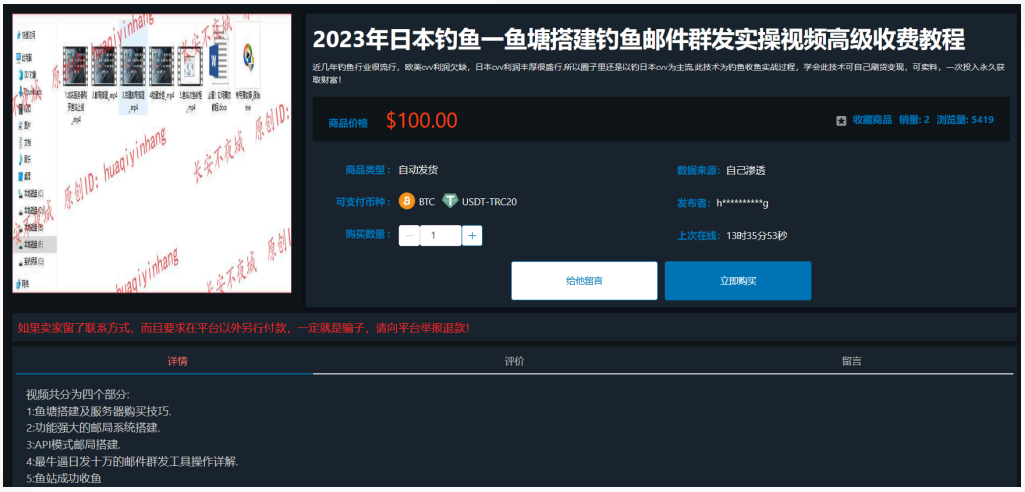
[13] https://www.anwangxia.com/2522.html

[14] https://www.anwangxia.com/2792.html

Alleged hand-held pictures of US driver's licenses with Social Security numbers (front and back images), offered for sale for USD 36 per item.

Alleged 400 Chinese passports offered for sale for USD 180.

Hacking tutorials are popular items for sale on this market. The following image is a listing with the price of USD 100 that claims to provide videos to teach beginners how to build a phishing website targeting Japan.

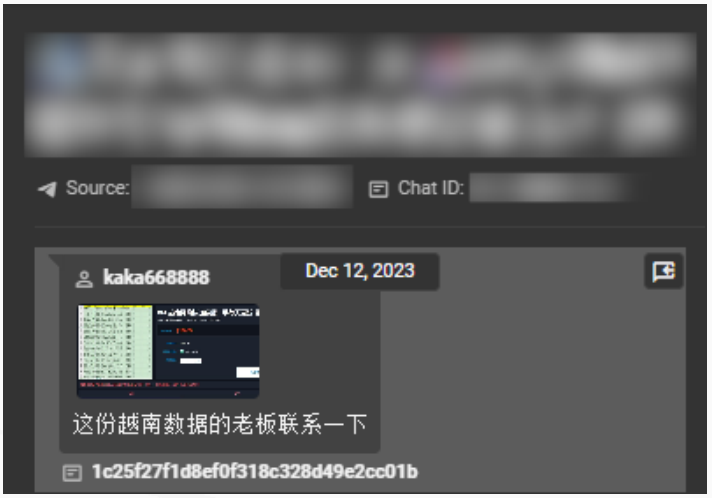


An alleged set of tutorial videos for building and using phishing toolkits targeting Japan is offered for sale on Market2.

The market allows payment via USDT, ETH, or BTC, and sellers can define the type of currency for purchasing the offered items. USDT-TRC20 seems to be sellers' most prevalent choice.

Recently posted items include Chinese domestic databases ranging from USD 10–130, foreign databases ranging from USD 100–500, fraud- and anonymization-related tutorials for around USD 100, "fast VPN" for USD 60, and ID pictures for USD 2–15 per item. It's important to highlight the extensive and varied database supply, though. As with Market1, various databases originating on the Chinese-based cybercrime markets are now more accessible and more easily circulated to the broader cybercrime and fraud communities through platforms like Telegram, making them easier to misuse.

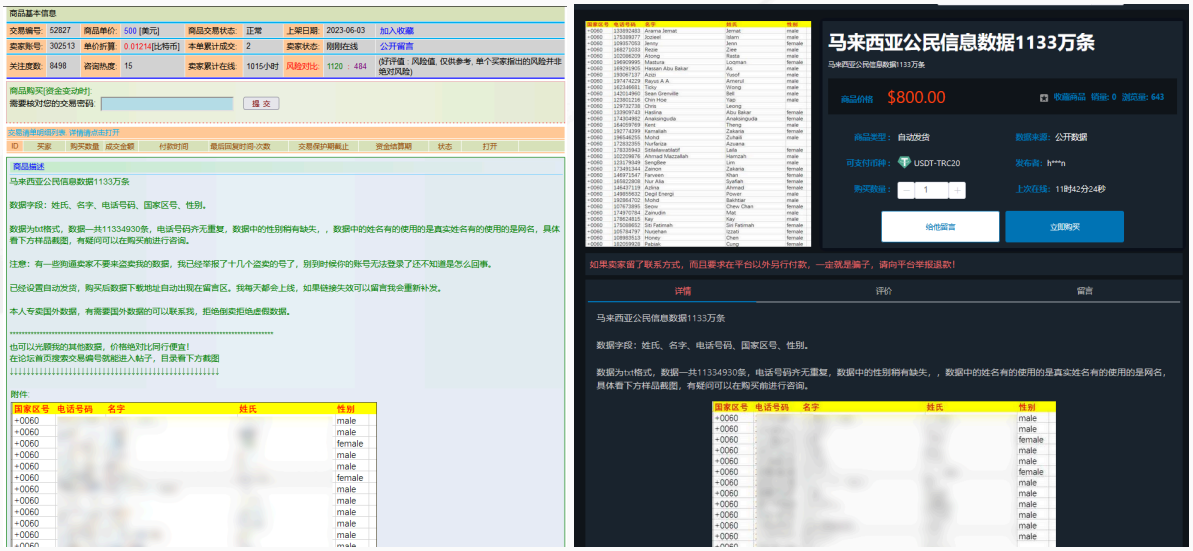
Market2's platform operation is supported with its official channels and discussion group on Telegram. The Telegram channel and group are managed by two admins, who are available for direct messages as well. The Telegram channel is mainly used for updates of the merchandise, and groups are used for users' communication with each other. For example, users can talk to sellers on the discussion group instead of using the comment section on the website.



A user kaka668888 posted on Market2's Telegram channel, asking the seller of the post in the screenshot from the market to contact them via Telegram.

Just like Market1, Market2 is not very well-equipped with user rating and quality assurance mechanisms. Similar to Market1, the usernames are hard to track: Instead of numbers, Market2 uses deducted usernames, such as "us*****e" instead of "username." Although there are sections for users to leave comments, reviews, and notes on each post, not many activities were observed there.

Additionally, per KELA's review, there are some actors on Market2 that repeatedly offer items listed on Market1 by different actors. The offers on Market2 are made a few days after the offers on Market1 are posted, and the prices are higher by 50% to 100%, yet the moderators and other users don't seem to intervene in such activities.



"Malaysian citizens' data 11,330K lines" offered for sale both on Market1 and Market2. The prices are USD 500 on Market1 and USD 800 on Market2.

Market2 is similar to Market1 in terms of its basic functionality, but it may be making a conscious effort to take over the position of what is almost its sole established competitor. Compared with Market1, for example, Market2's Telegram group may be complementing lack of activities on the market itself: Users can expose users who engage in fraudulent transactions or postings on the group, or actively communicate on the group to earn trust. Market2's operators mentioned Market1 negatively multiple times in the update section on its landing page and in its Telegram channel, not hiding its hostile rivalry toward the older platform. Also, while Market1's trade currency is limited to BTC, Market2's support for transactions in multiple currencies may be more suitable for modern users.

Currently, both markets are attempting to survive in their competition, though in this case their future existence depends less on their rivalry than on whether they can manage to stay and grow despite the increasing popularity of Telegram.

Telegram fraud ecosystem

Per KELA's research, Chinese-speaking cybercriminals are active in channels and groups on instant messaging services. In particular, it appears that hackers and criminals may consider Telegram to be safer from censorship by the authorities than Chinese messaging apps such as WeChat.

WeChat, provided by the Chinese tech giant Tencent, is the most dominant instant messaging app in China and among Chinese users.

QQ, also provided by Tencent, used to be a popular messaging app but is now available only as a mobile instant messaging app.

Telegram is a messaging app used by many people around the world for a variety of purposes. However, it has also become a hub for cybercrime activities, including the sale and leakage of stolen personal and corporate data, the organization of cybercrime gangs, the distribution of hacking tutorials, hacktivism, and the sale of illegal physical products such as counterfeits. In addition to direct messaging between individuals, Telegram has channels and groups. In a channel, only the channel admin can post content, and subscribers can only view it or contact the admins directly. In a group, all members are allowed to post. Both channels and groups can be invitation-only, but there are also many channels that contain illegal content that are made public for popularity.

As Tencent operates WeChat and QQ in compliance with China's data and cybersecurity laws, Chinese cybercriminals may refrain from engaging in criminal activities through these apps due to lack of anonymity and privacy. The operators of Market2, for example, advise its users to steer clear of Chinese domestic messaging apps such as QQ and WeChat. Instead, they emphasize leveraging foreign platforms, particularly their designated communication channel and discussion group on Telegram:

> «*4. At the same time, this site, except for the advertising area, does not encourage (users) to contact outside the site. If, due to the functional limitations of the platform, users must contact each other outside the site, then please use the foreign company's communication tools, do not use QQ, WeChat, etc.*
> *(4.同时，本站除广告刊登区外，都不鼓励站外联系,如因平台功能受限的情况不得不站外联系，那请大家使用外国公司的通联工具，不要使用QQ、微信这类软件。)*»

KELA identified various Telegram channels and groups operated in Chinese and dedicated to cybercrime activities. These groups and channels discuss topics of an illegal nature, such as penetration-testing services, sales of stolen databases and credit-card information, methods of money laundering, fake and stolen IDs, tutorials, and so on.

The Chinese-speaking criminal activity in Telegram usually takes place in channels, groups, and customer-service accounts set up by the providers of Illicit services and items, most likely to run their business in an organized manner and gain effective marketing exposure:

- Channels are used for the operators to announce updates about their merchandise and services, and notes for their customers.
- Groups are used for buyers, users, and potential customers to freely post anything relating to the theme of the group.
- Customer-service accounts are used for support of buyers. Some groups replace this role with a bot that deals with orders, FAQ, and transactions automatically.

KELA observes that many actors who provide services routinely post their advertisements in many similar themed groups, and other group operators seem to allow it. For such reasons, groups often attract more users than channels and serve as an entry point for operators to attract more people to their channels.

The Chinese-speaking cybercriminals have a unique set of manners they use in Telegram. Despite that often admins even specify the groups as "chat groups", Chinese-speaking groups of an illegal nature are often used almost as if they were old-style bulletin boards. Admins often use the community to publicize ad posts for their offerings, which usually accompany a link to another channel where more information is available. Such posts are pinned in the group so the ad will be seen by anybody who is interested in the topic and takes a glance at the group by chance. Other members leave minimalistic posts of offers and demands accompanied by their Telegram account for contact, and discussions among members often occur through direct messages.

For example, the following image is a screenshot of a Chinese Telegram group dedicated to illicit IDs, showing different users leaving messages about the items they're offering, such as driver's licenses, passports, and Social Security numbers.

Users leave short offers or demands in Chinese-speaking Telegram groups.

Also, Telegram channels and groups are one way for the operators and users to report untrusted users. Some admins expose transactional frauds in their own channels and groups. Many channels and groups are specifically dedicated to accusations of fraudulent actions in the cybercrime communities cross-platform (not only in Telegram).

KELA has chosen several operations managed through Telegram per different topics to illustrate some of the Chinese-speaking activities on the platform.

Hacking-as-a-service

Hacking-as-a-service is a popular form of cybercrime activity, and many Chinese-speaking service providers operate on Telegram.

Per KELA's review, hacking-as-a-service can be often described as "penetration-testing service" (渗透 服务), with popular subtypes including "database breach" (脱库) and "website takeover" (拿站). Website takeover refers to the successful hacking of a website with admin access and control of the backend system.

While the end results of these activities – such as initial network access via VPN or access to the website management – are openly exchanged on English- or Russian-speaking cybercrime forums, Chinese-speaking cybercriminals may prefer to only advertise their services. Per KELA's observation, in the Chinese-speaking cybercrime forums, such explicit sales of network or website access are less commonly spotted, though databases are still the popular product.

Use case: Channel1

The Telegram channel Channel1 has been active since April 2023, and as of January 2024 it had more than 9,000 subscribers. The channel's operators allegedly provide database-breach-as-a-service, predominantly by exploiting SQL injection vulnerabilities. Its channel description outlines a three-tier pricing structure, depending on the industry. "Education, forum, and school campus" compromise starts at RMB 20,000 (roughly USD 2,800). "Finance, recruitment, and securities" compromise is priced at RMB 30,000 (roughly USD 4,300). "Gambling, shopping, and material station," which refers to illegitimate websites that offer stolen items for sale, compromise starts at RMB 50,000 (roughly USD 7,000). The description also claims that service will be provided within 15–30 days after receiving an order.

Credit card data – CVV

Deals for stolen card information, either credit cards or prepaid cards, are one of the major activities prevailing in the Chinese cybercrime ecosystem. The overall circulation of stolen card information is neatly divided by dedicated providers and buyers of services, items, data, and tools for stealing, filtering, monetizing, and laundering.

"CVV" originally meant the type of stolen card data that includes the CVV number, to describe merchandise that was more valuable than stolen card data without the CVV number, back when the main source of such data was less sophisticated physical card skimming via ATM and POS.

Now, however, the Chinese cybercrime ecosystem uses “CVV” to refer to carding (illegitimate deals for stolen card information, including credit, debit, etc,) as a crime-market genre. Nowadays, card information without the CVV number can still be offered in such channels and is often described as “无C,” meaning “No CVV number.”

Additionally, many channels are focused either on domestic Chinese data or data from other countries, and seldom are these two target markets mixed. Some actors operate two or more channels per target market.

A Chinese-speaking CVV channel advertising Japanese credit-card data and Amazon account credentials, allegedly with 3D secure code, most likely stolen via a phishing website impersonating a legitimate Amazon Japan website.

Example of daily/weekly in-stock BIN list.

Use case: Channel2

Channel2 is one of numerous channels and groups operated in Chinese that mainly engage in deals for stolen card data. The operation has been active since July 2023 and includes an official channel with more than 5,000 subscribers, Telegram accounts dedicated to "official customer services," and a Telegram group called Chatting on CVV, which has over 7,000 members.

The channel description claims that this provider deals with global card information, focusing especially on Japan, Hong Kong, Taiwan, Australia, South Korea, the Philippines, Thailand, Canada, Argentina, and South Africa. It claims to have card information procured both by phishing and from leaked databases, and occasionally drops "welfare material" (福利料), which means free samples.

The channel's business operation is simple. The operator posts an updated list of bank identification numbers (BINs) that are in stock for sale. Interested buyers can contact the customer service account and request data on specific BINs or random BINs in specific countries in a selected amount. The list of BINs can be labeled as "Japan BIN – 80% checked as effective" or "Global mixed BIN – 99% checked as effective."

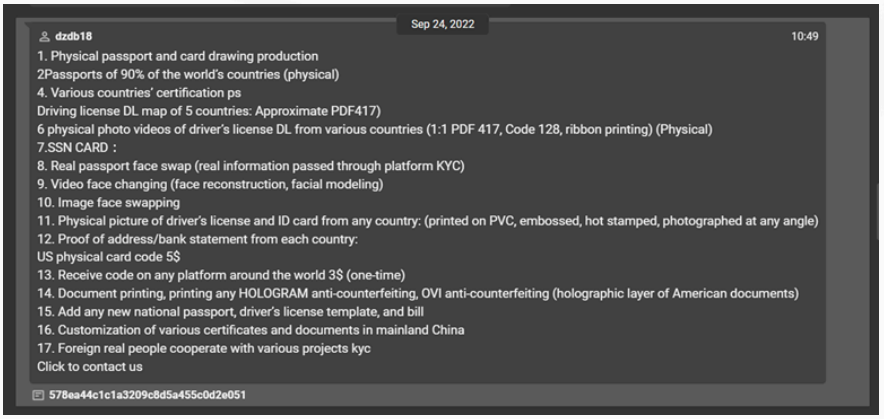
As aforementioned, in the group the users can discuss trends and services and post memes, but most often they leave inquiries or notes to advertise their own business.

Counterfeit IDs – "KYC," "P," and "证" certificate

Counterfeit IDs are another major merchandise category in the Chinese cybercrime ecosystem and an inherent part of the broader card fraud ecosystem. This category deals with fake IDs, stolen authentic IDs, and pictures (image data) of them.

One popular item is called "KYC" (手持 – literally, "hand-held"). These are images of individuals holding their real ID next to their face. KYC, short for "know your customer," is a common way for users to prove identification when registering an account for legitimate services, such as banking.

Fraudsters use the KYC process on phishing websites. Criminals use the images of victimized individuals for various reasons, but especially as part of larger card fraud schemes, combining them with CVV data to "cash out" or launder money.



A post on the Channel3 channel by the admin describing the alleged available services (auto-translated on KELA's platform)

Use case: Channel3

One of the providers of illegitimate IDs is a project called Channel3. The Telegram group was created in September 2022, and now it has around 200 members.

The group's profile doesn't contain a description but indicates a location in the Philippines. As the profile picture suggests, this is a side project of an actor called 大众担保, which can be translated literally as "Broad Public Guarantee (service)" or colloquially as "Volkswagen guarantee." The admins run another channel dedicated to KYC materials that has over 1,300 members.

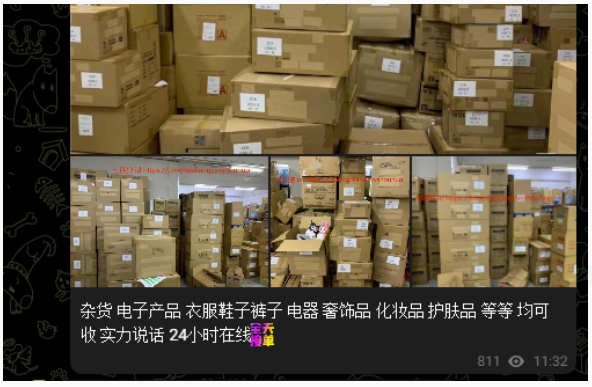
The channel operator claims to provide almost any type of certificate, or at least a photocopy of it, from almost any country. The list includes physical passports, driver's licenses, Social Security cards, proofs of residential address for various countries, printed counterfeit documents that are hologram-proof, and foreign KYC documents of "real" people outside of China. The list also includes a "face-swapping" service, which per KELA's review may refer to changing the picture in an image of an authentic ID.

"Cashing" services (收货, 变现)

Many Chinese-speaking Telegram channels deal with "cashing" and money laundering services. Cashing is the final stage of monetizing various financially motivated cyber frauds.

Use case: Channel4

The Channel4 Telegram channel provides cashing services in the card fraud ecosystem. The operators of the channel claim to engage in regions including Canada, Japan, and Hong Kong. They state in the channel description that they will buy products that fraudsters purchase using stolen credit-card information. This allows the fraudster to get cash or other currency that they can freely use. According to the description, the products they'll buy include such things as home appliances and alcoholic beverages. From the posts, it appears that they also resell the purchased products.



A post by the channel admin of items including electronic appliances, clothing, and cosmetics, allegedly purchased from channel users who delivered them by stolen account and credit card in exchange for money. The admin claims to resell the purchased items.

Bypass services

KELA notes one type of Chinese cybercrime activity prevelent on Telegram that facilitates informal currency exchanges and the trade in illicit items and services, especially the ones related to bypassing Chinese laws on Internet use. One example is the Telegram channel called Channel5, which has over 26,000 subscribers.

Such groups may enable Chinese-speaking users to buy cryptocurrency without using their own ID, as required by the Chinese government, or to access VPN services, which are banned in China. They also may enable users to buy fake SIM cards and use overseas phone verification services to help protect their identities.

Chapter summary

KELA's investigation into the Chinese-speaking cybercrime ecosystem has discovered a multi-layered structure with distinct roles and functionalities. Significantly, the shift toward Telegram is a pivotal component of this ecosystem. The platform has transcended traditional web-based markets and forums, evolving into a hub for communication and coordination among threat actors.

The rationale behind the increased reliance on foreign apps, such as Telegram, is linked to the tightened restrictions on anonymous Internet usage. Chinese-speaking actors, adapting to these constraints, are increasingly favoring foreign apps over domestic ones. This strategic move underscores the adaptability and resilience of the cybercrime community in navigating regulatory challenges.

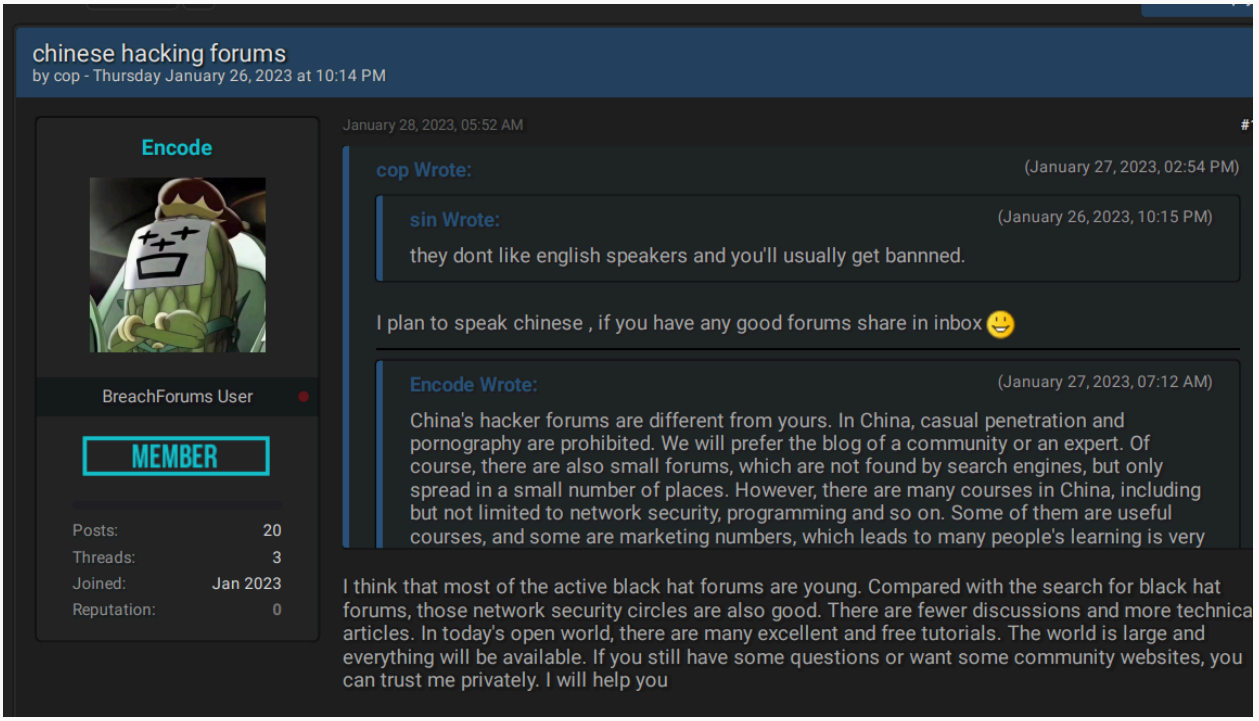
It's crucial to recognize that the impact of Chinese-speaking hackers extends beyond their dedicated platforms. In the upcoming chapter, KELA will show the integration of these hackers, those from or associated with China, into non-Chinese-speaking hacking community websites.

Chinese-speaking actors on non-Chinese platforms

Chinese-speaking hackers have a presence on the non-Chinese-speaking hacking community websites and use the tools that circulate there. The evolving cybercrime underground is increasingly servicing and automating related activities, accelerating the trend of cybercriminals being location- and language-agnostic. On the English- and Russian-speaking platforms, KELA has observed many users who communicate in Chinese along with other languages.

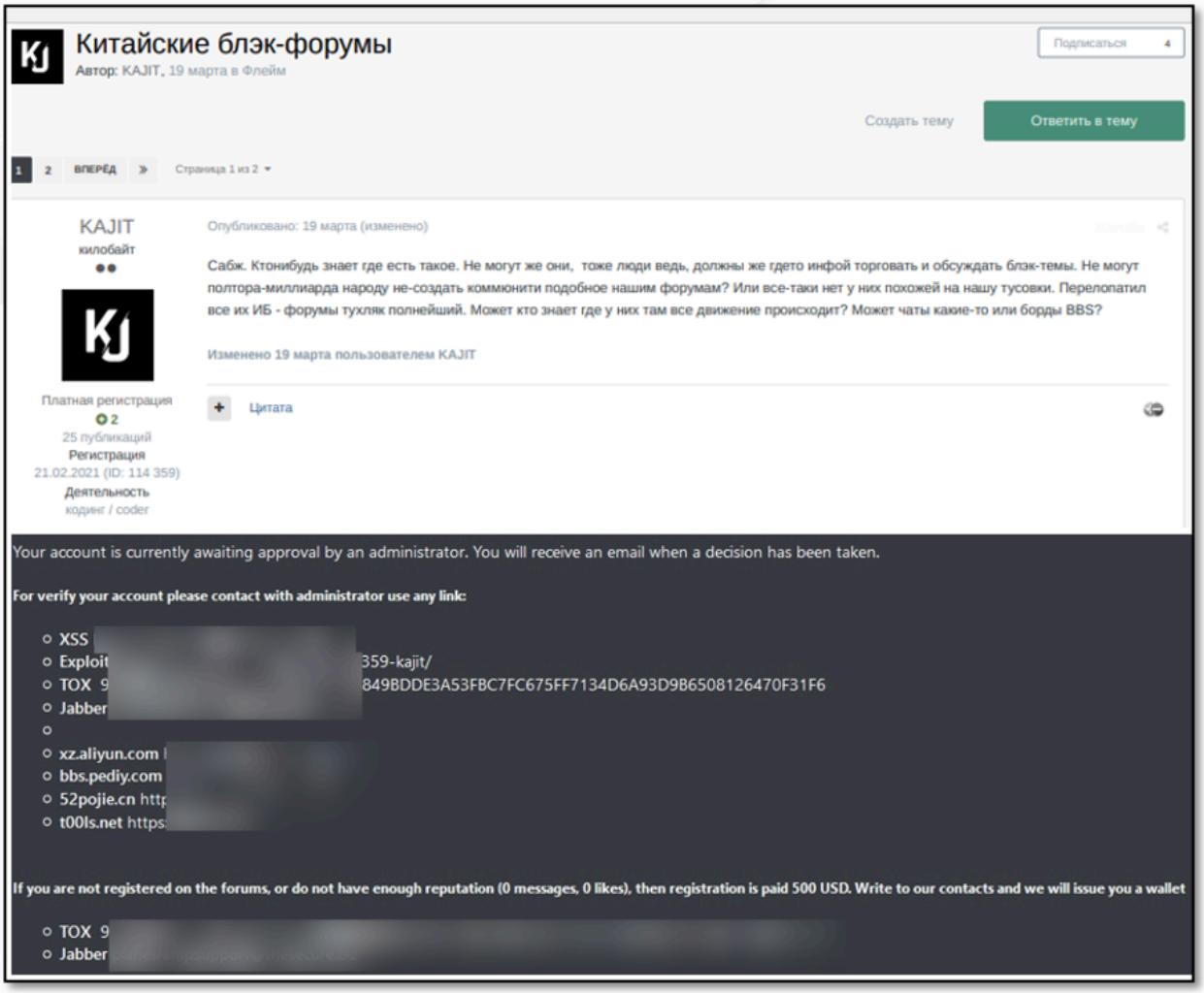
Non-Chinese platforms' efforts to bring Chinese-speaking cybercriminals

Interestingly, some communities have invested in attracting Chinese-speaking cybercriminals, deeming them skilled enough to benefit such communities, while some users have shown interest in Chinese-speaking communities.



Actors are discussing Chinese hacking forums.

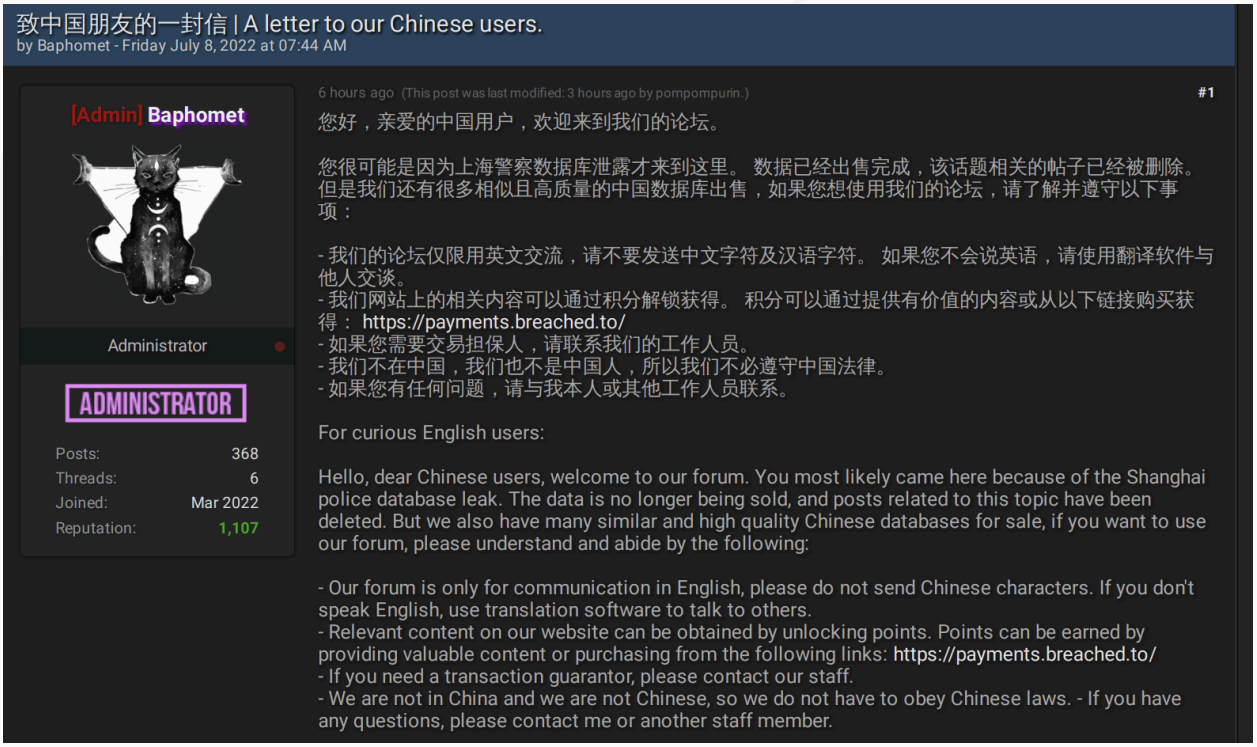
For example, in November 2021, the threat actor KAJIT launched a cybercrime forum named RAMP, intended to attract both Russian-speaking and Chinese-speaking actors. Before launching the forum, KAJIT showed a high interest in Chinese-speaking platforms and their users.



In March 2021, KAJIT was seen looking for Chinese forums. In November 2021, when registering on the RAMP forum, a user gets recommendations to several Chinese forums from KAJIT.

The forum's interface was partially translated into Chinese. Now, after KAJIT leaving the RAMP, Chinese-speaking users seem to still be present on the forum, though in general the forum stayed mostly Russian-speaking. This attempt shows that some Chinese-speaking users are open to interacting with their international colleagues.

A wave of Chinese-speaking users appeared on different forums in June 2022, following the sale of a database allegedly belonging to the Shanghai National Police that was first advertised for sale on RAMP by the user ChinaDan. The same day, the same offer was made on the Russian-speaking forum Exploit by an actor called AccessBroker. A few days later, ChinaDan posted the same offer on BreachForums. The database got a lot of attention from users, and its popularity even caused the BreachForums admin to write a welcome message for newly registered Chinese users searching for the leak.

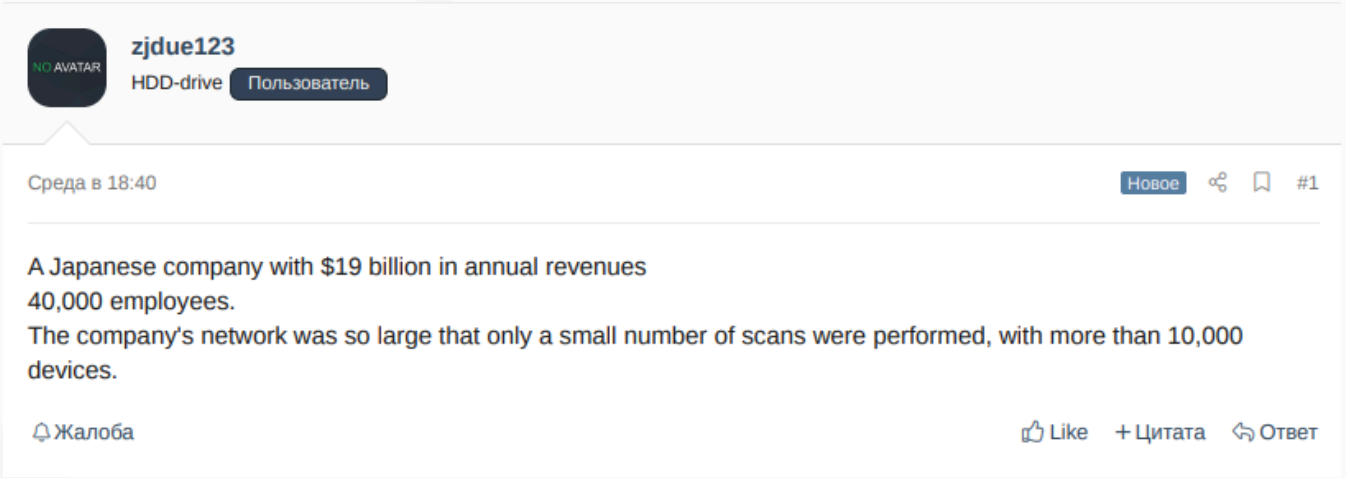


A welcome message for Chinese users written by Baphomet, a BreachForums admin, in 2022.

KELA has chosen several Chinese threat actors who are active on Russian- and English-speaking forums to illustrate their involvement. The actors were defined as Chinese-speaking cybercriminals following KELA's analysis of their activity and engagements.

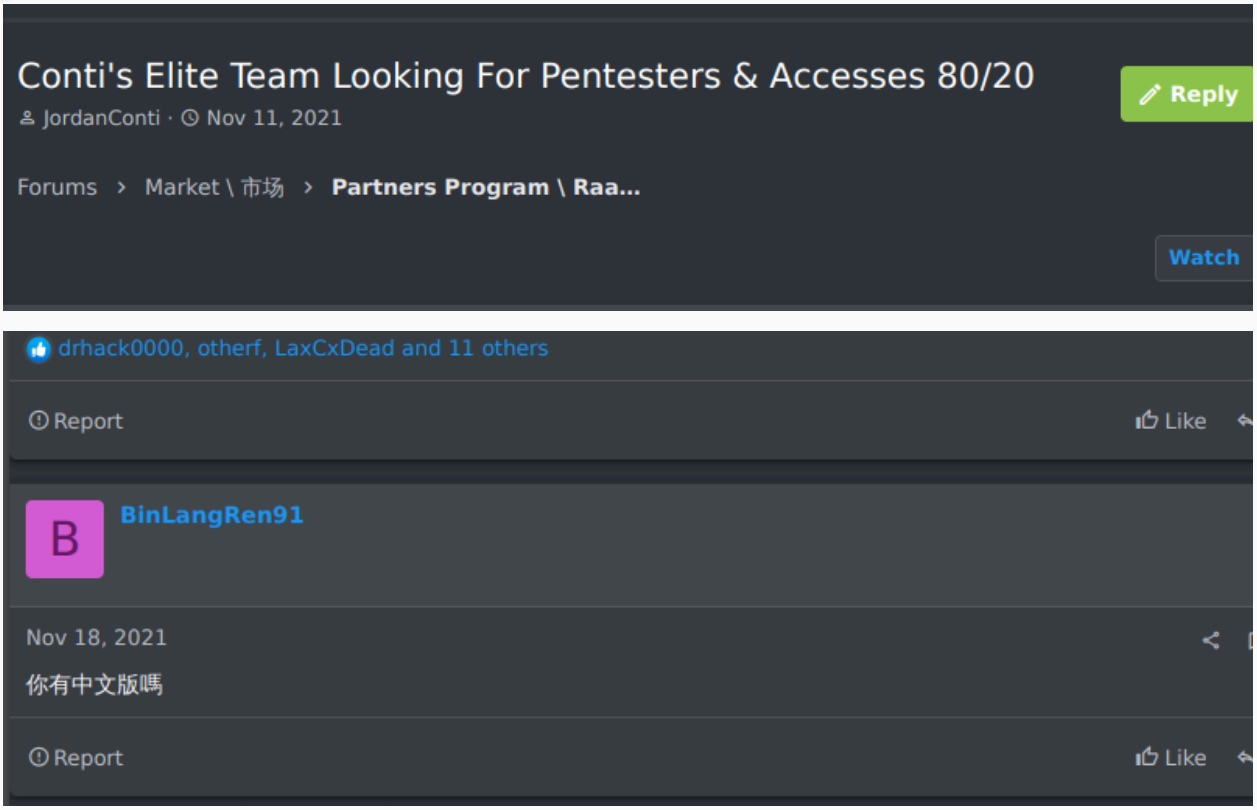
Chinese-speaking actors on non-Chinese platforms

The Chinese-speaking threat actor zjdue123 has been active on XSS since June 2020. Over the years, the actor has been recruiting penetration testers, acting as an initial access broker (such as selling access to a Japanese company) and chatting on Chinese-related matters, as well as participating in general discussions.



The actor is selling network access to a Japanese company with USD 19 billion in revenue.

Another Chinese-speaking threat actor, Binlangren91, has been active on RAMP since November 2021, demonstrating interest in ransomware-as-a-service. For example, the actor also replied to an ad by Conti operators who were looking for penetration testers and initial access brokers, asking whether there is a Chinese version (probably the actor misunderstood that the group was looking for affiliates).



"Do you have a Chinese version?"

Multiple other Chinese actors noticed by KELA have been mainly interested in buying databases, with some of them being focused on several regions, such as an actor looking for Southeast Asian databases.

The actor Au4au410 is interested in Hong Kong databases.

Chapter summary

KELA has observed the emergence of Chinese threat actors on both international and Russian-speaking cybercrime forums. This trend involves collaboration and ongoing cooperation between different threat actors, who bring diverse skills, tactics, and motivations, making it more challenging to defend against cyberattacks. It also contributes to circulation of leaked information across Chinese-speaking and other communities, with unique information from both sides being reshared on other platforms.

Moreover, it can be assumed that members of APT groups have vast access both to a Chinese-speaking and wider cybercrime ecosystem. In the upcoming chapter, KELA will focus on evidence suggesting that Chinese APTs have been exploiting various resources over years, acting as typical sophisticated cybercriminals.

Chinese APTs and cybercrime platforms

APT groups are skilled threat actors that are known to be well-resourced and that conduct highly sophisticated and targeted campaigns against their victims. These groups often develop their own custom malware and tools. However, APTs are also known to use commodity and open-source tools, which can be obtained online.[15]

Chinese APTs, while known to develop custom malware, have also been observed using publicly available tools, which they may modify to meet their requirements. There are various reasons why an APT group may choose non-custom tools for an attack, including:[16]

- **To evade defenses:** The use of open-source or malware-as-a-service products adds an extra layer of obfuscation for APT groups because other threat actors, or even legitimate penetration testers, also use these tools. This makes it harder for security researchers to attribute campaigns to an APT group.
- **To save time and money:** The development of custom malware is time-consuming. By using existing tools, APT groups can save on time and development costs.
- **To fill a gap:** These groups might not have custom tools for every stage of an attack, so they turn to open-source tools – for instance, for reconnaissance purposes – before deploying their custom tools.

Below are some examples of publicly available tools used by APT groups believed to be linked to China.

Budworm uses variety of open-source tools

In June 2023, researchers reported that they identified a malicious web server, which they believe was likely operated by a Chinese threat actor primarily to target Taiwanese government organizations. The researchers noted that the identified tactics, techniques, and procedures overlapped with the Chinese APT group Budworm.[17] The threat actor used a variety of open-source tools, including some that are believed to be available only from Chinese sources.

Among the tools identified being circulated in Chinese sources was Cobalt Strike Cat, a modified version of Cobalt Strike 4.5, a commercial penetration-testing product that has become popular among threat actors. Numerous Chinese APT groups are known to have used Cobalt Strike in their campaigns.

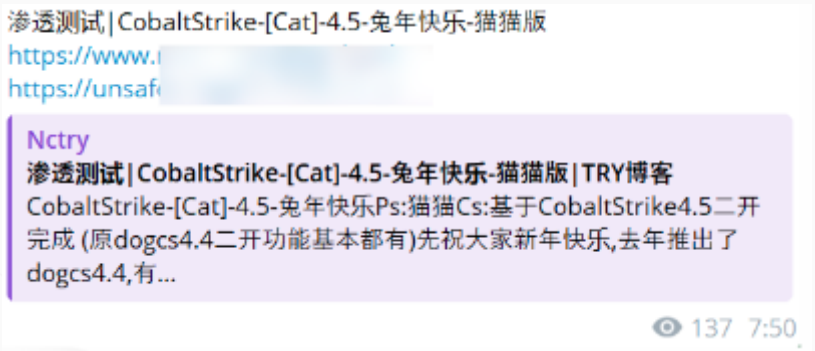
[15] APT Groups and Their Presence in the Cybercrime Ecosystem

[16] APT Groups and Their Presence in the Cybercrime Ecosystem; Nation-State Hackers Go Open Source

[17] Chinese Threat Actor Used Modified Cobalt Strike Variant to Attack Taiwanese Critical Infrastructure

Actor selling a Cobalt Strike license.

Cobalt Strike Cat is available on GitHub. However, a decryption password is needed for the zip folder with the tool; the password was shared on t00ls, a Chinese network security community.[18] Only registered users with certain permissions could obtain the decryption key.[19] Users need an invitation code to register for an account and must submit an original article or identified vulnerability. KELA also observed the link to the GitHub author's blog post on Cobalt Strike Cat being shared on Telegram.



Link to a blog post about Cobalt Strike Cat shared on Telegram. The blog post provides the link to the GitHub page.

The threat actor also used ONE-FOX, a collection of penetration-testing tools. ONE-FOX was shared on the Chinese blog ddosi.org and appears to have been shared originally on WeChat, where users needed to message to receive the download link.

[18] CobaltStrike_Cat_4.5

[19] Chinese Threat Actor Used Modified Cobalt Strike Variant to Attack Taiwanese Critical Infrastructure

Advertisement for ONE-FOX on WeChat.

APT10 uses modified versions of Quasar

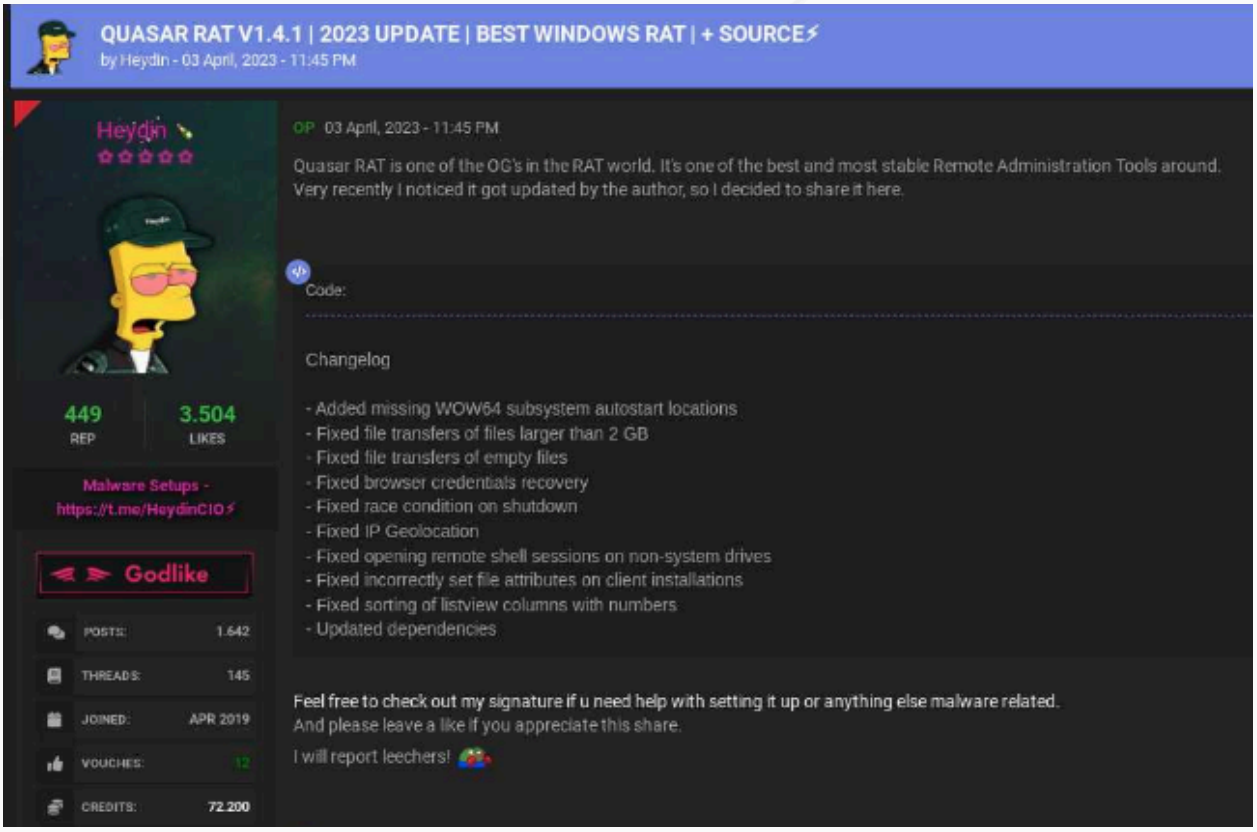
Quasar is an open-source remote administration tool (RAT) for Windows that is publicly hosted as a GitHub repository.[20] The tool was first released in 2014 under the name xRAT 2.0, before being renamed to Quasar in 2015.

Quasar has been highlighted as a good open-source RAT in cybercrime forums, and links to GitHub, where it's available for download, have been shared. Modified versions of Quasar have also been circulated in cybercrime forums, either for free or for sale. APT groups have been identified using Quasar, including modified versions that they're believed to have customized to accommodate their specific needs.[21] APT10, a Chinese threat actor group that is believed to have been active since 2006, has used its own customized versions of Quasar since at least 2016-17.[22]

[20] Quasar

[21] Quasar Open-Source Remote Administration Tool

[22] APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat



An actor shares one of the recent Qasar versions

APT1, Gallium, Mustang Panda, and APT10 use Poison Ivy

Various Chinese APTs have been observed using Poison Ivy, or modified versions of it, in their campaigns. Poison Ivy is a remote administration tool with various functionalities, including key logging, screen capturing, and webcam viewing. Chinese groups that are known to have used it include APT1,[23] Gallium,[24] Mustang Panda,[25] and APT10.[26]

Poison Ivy is believed to have first been released in 2005. It had been available for download for free off their dedicated website, where numerous versions of the malware were shared. Actors in cybercrime forums were observed sharing the link to the Poison Ivy website, and KELA also identified versions of Poison Ivy being shared in cybercrime forums as an individual tool or as part of a hacking toolset. The developer doesn't appear to have publicly updated the tool since 2008, and the Poison Ivy website is no longer available. However, versions of Poison Ivy are still being circulated in cybercrime forums, with the most recent identified from KELA's sources being shared in June 2023.

[23] APT1

[24] GALLIUM: Targeting global telecom

[25] MUSTANG PANDA

[26] menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations

Poison Ivy website (captured in June 2014)[27]

Chapter summary

Chinese APT groups are known to use custom-developed malware in their attacks. However, they're also known to use publicly available tools. These include legitimate tools, such as penetration-testing and remote administration tools, that these groups have leveraged for malicious purposes. Chinese APTs have also been observed building their custom malware off publicly available tools.

The publicly available tools used by Chinese APT groups can be found circulating in various sources, including WeChat, GitHub, and network security communities (specifically t00ls), and on their own dedicated websites. Tools were also observed being reshared in cybercrime forums. The presence on WeChat and t00ls of tools used by Chinese APT groups confirms KELA's wider findings that Chinese-related activity can be identified on Chinese online resource-sharing platforms.

The fact that Chinese APTs are using these non-custom tools demonstrates that these groups are looking to acquire tools online and are likely accessing various sources to acquire them.

[27] https://web.archive.org/web/20061105020002/http://www.poisonivy-rat.com/

Conclusion

In conclusion, the Chinese cybercrime ecosystem exhibits a unique combination of characteristics, comprising both Chinese-only sources, primarily on Telegram and Chinese resource-sharing platforms, and participation by Chinese actors in well-established English- and Russian-speaking communities. The distinct features of Chinese-speaking cybercriminal activity can be summarized as follows:

- **Indirect and discreet approach:** Chinese-speaking cybercriminals adopt a more indirect and discreet approach in discussing and exchanging information, compared with their counterparts. This may be due to fear of detection by the authorities and heavily affects their methods of communication and manners of engagement in the cybercrime ecosystem.
- **Focus on services and offers instead of discussions:** Sticking to their discreet approach, the content that Chinese-speaking cybercriminals share across various platforms is predominantly focused on services and offers rather than discussions and often uses coded language or a general overview instead of specific offers. Following this, Chinese-speaking actors often provide services that aren't that popular in other communities, such as database breach per request. This contrasts with English- and Russian-speaking cybercrime communities, where a mix of discussions, specific offers, and direct descriptions is more common.
- **Lack of established reputation systems:** In contrast to other communities, Chinese actors often operate without well-established reputation systems, prioritizing the anonymity of users. Trust is primarily built through direct messages.
- **Lack of web-based communities that openly offer cybercrime tools, services, etc.:** Chinese-speaking cybercriminals operate only in several distinct web-based communities, with all of them working as a board or market and not as a fully functional forum. This deviation adds another layer to their discreet and indirect approach.
- **Scarcity of cross-platform business:** Chinese-speaking cybercriminals differ from their counterparts by rarely being active on different platforms under one handle or operation alias. Unlike other cybercriminals who maintain a presence on various cybercrime forums, markets, Telegram, etc., to sustain their reputation and availability, Chinese actors exhibit a more focused and streamlined approach.

As for the similarities and integration of Chinese-speaking cybercriminals into the overall cybercrime ecosystem, several key points emerge:

- **Heavy reliance on Telegram:** Similar to other cybercrime communities, Chinese-speaking cybercriminals heavily rely on Telegram as a primary platform for their operations.
- **Dedicated platforms trend:** Chinese-speaking cybercriminals mirror the trend observed in other cybercrime communities, where dedicated platforms cater to specific activities. However, in their case, the focus is primarily on Telegram rather than web-based autoshops and marketplaces.
- **Presence in multiple language communities:** There's a notable presence of Chinese-speaking actors who also operate in English- and Russian-speaking cybercrime communities, potentially leading to a wider distribution of leaked information and cybercrime tools.
- **Integration of APT members:** Chinese-speaking APT members, alongside counterparts from other regions, actively benefit from the diverse cybercrime ecosystem. These actors are likely engaged in buying and using information and tools from the underground markets to facilitate their sophisticated attacks.

Understanding these nuances is crucial for effective threat monitoring across different platforms. Having access to both Chinese-only and English- and Russian-speaking platforms is essential for cybersecurity professionals to stay a step ahead of cybercriminals.