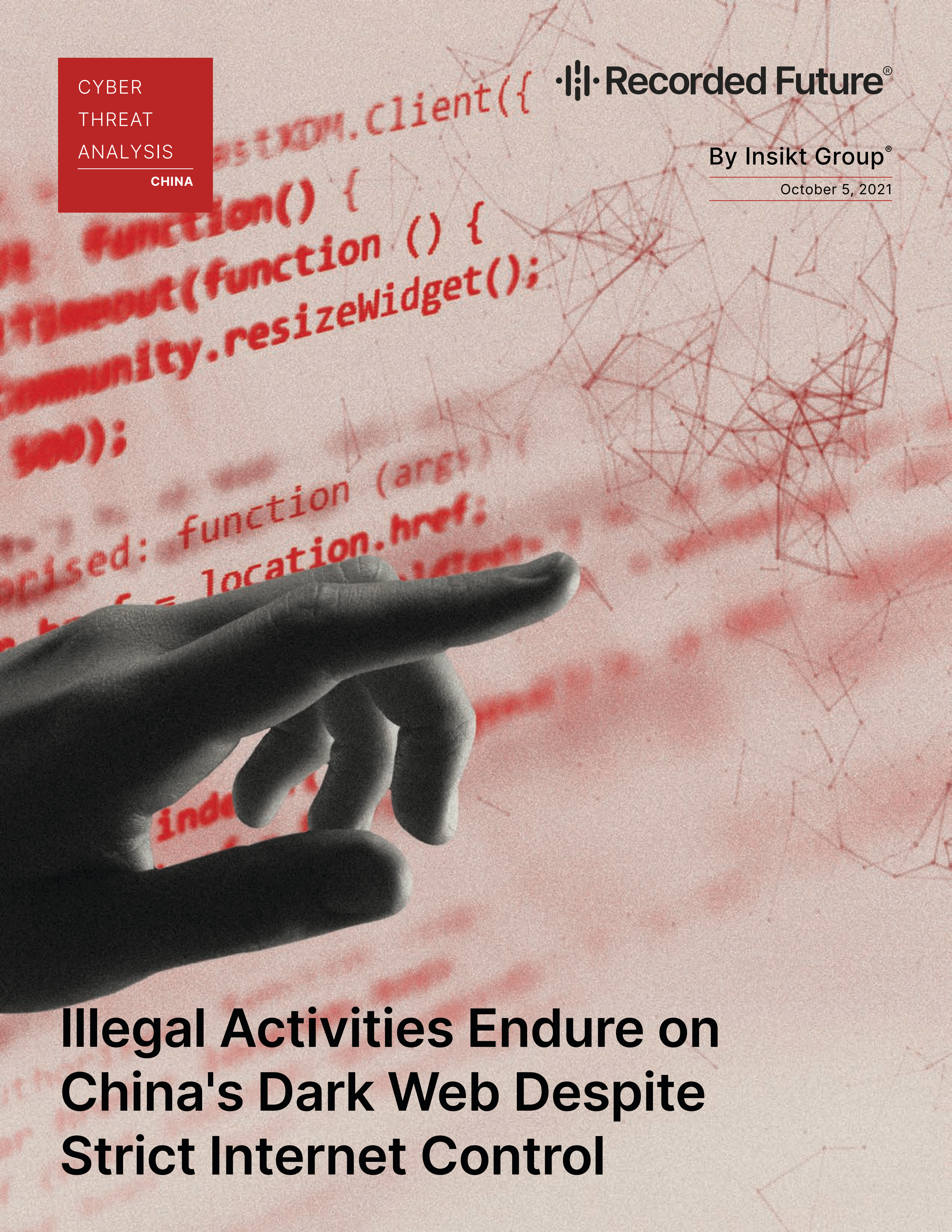
CYBER
THREAT
ANALYSIS
CHINA

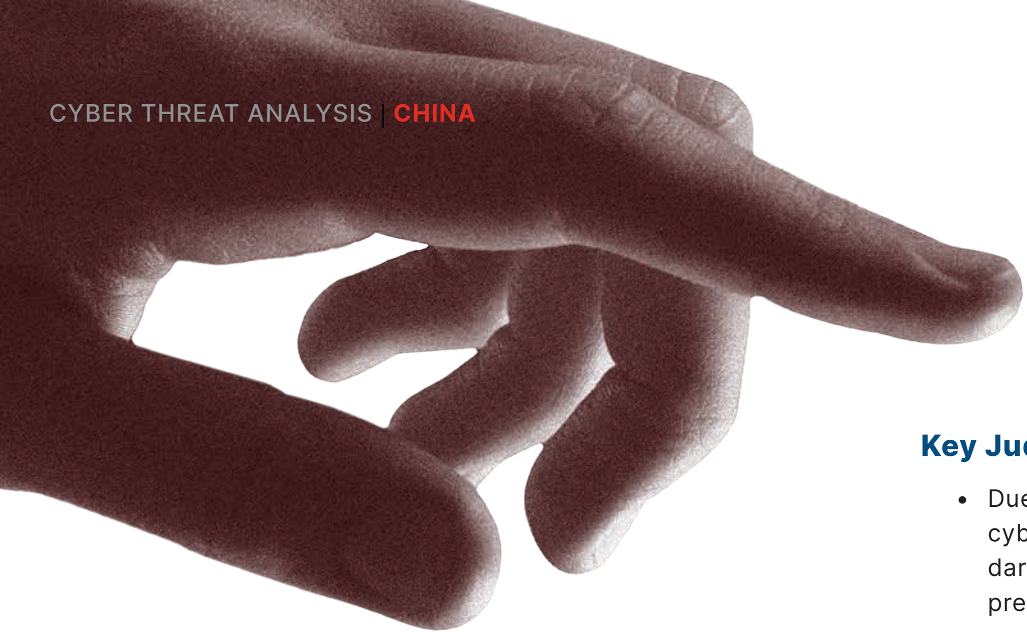
Recorded Future®

By Insikt Group®

October 5, 2021



Illegal Activities Endure on China's Dark Web Despite Strict Internet Control



This report analyzes the structure of internet sources used by Chinese-speaking threat actors to facilitate cybercriminal activities, specifically Chinese-language dark web sources, clearnet hacking forums and blogs, instant messaging platforms, and well-established criminal sources. This report aims to provide a general understanding of the Chinese-speaking cybercriminal landscape and the threat it presents under the context of its distinct cultural, political, and legal characteristics. Findings in this report include results from the Recorded Future Platform® and dark web and open sources.

Executive Summary

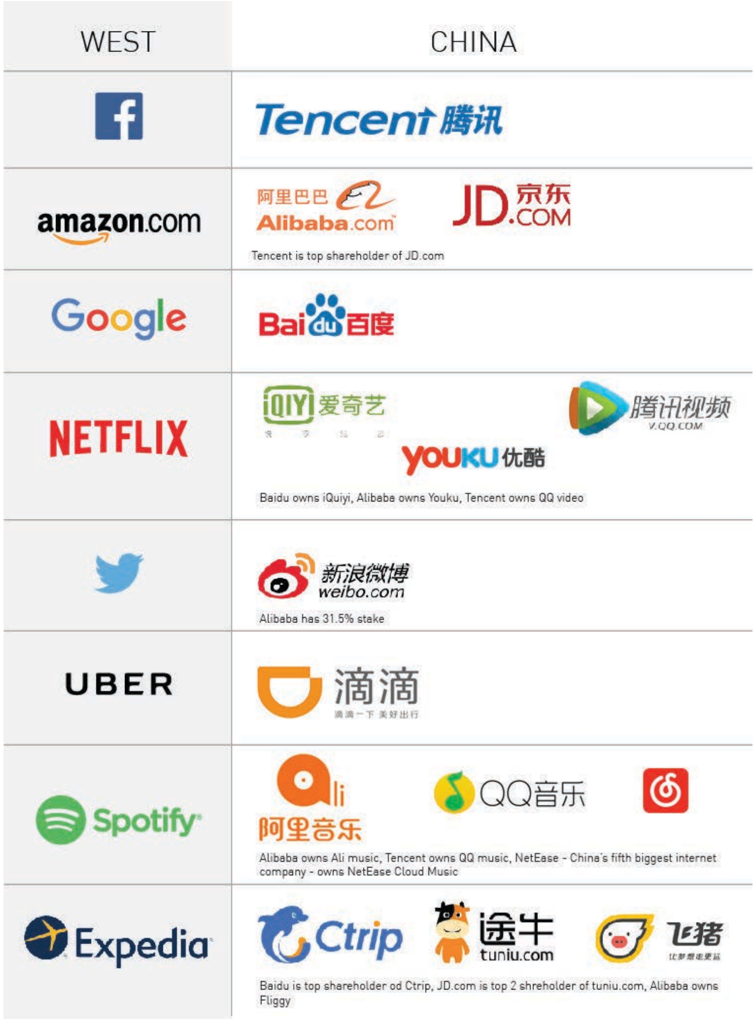
Chinese-language dark web sources are predominantly driven by financially motivated cybercriminals operating on marketplaces. Due to the government's low tolerance of cybercrime and frequent crackdowns, maintaining good operational security and anonymity is essential for these cybercriminals. Although there is a wide variety of offerings in the Chinese-language dark web marketplaces, they are generally dominated by leaked data and virtual goods, which are easy to buy and sell while remaining anonymous. For the same reason, Bitcoin is the dominant currency on these marketplaces, and the marketplaces are generally integrated with messaging platforms, particularly Telegram. Due to constant law enforcement actions, lower-tier marketplaces commonly shut down and reopen; some of the more experienced threat actors are possibly migrating to international, well-established dark web sources to conduct business. The Chinese-speaking cybercriminal underground will almost certainly find ways to survive and thrive despite government crackdowns, however.

Key Judgments

- Due to frequent government crackdowns on cybercrime, offerings on the Chinese-language dark web marketplaces are dictated by the preservation of anonymity. As a result, virtual goods such as compromised data and tutorials are the most popular products as they can be delivered anonymously online. Due to the need for delivery to physical addresses, physical goods such as weapons and drugs, widely offered in other cybercrime ecosystems, are less common in China.
- Unlike Russia and other cybercriminal ecosystems where domestic entities are not targeted, the offerings on the Chinese-language dark web marketplaces are dominated by domestic offerings. Advertised items can range from exfiltrated data from China-based financial conglomerates to gambling and loan applications (apps). This could be due to the large domestic attack surface and the relative ease of access without the need to get around the Great Firewall of China.
- Compared to mature cybercriminal ecosystems such as those in Russia, the Chinese-language underground lacks a hierarchical structure. Highly collaborative and structured ransomware affiliate programs or infostealer malware-as-a-service (MaaS) programs are absent. In addition, the general lack of trust between cybercriminals as well as between cybercriminals and marketplace operators further prohibits such collaboration. For this reason, cybercrime know-how is often monetized and passed along through tutorials instead of personal working partnerships.
- China-based threat actors with foreign language skills, hacking skills, and access to exfiltrated data are migrating toward established international cybercrime forums as well as messaging platforms due to concerns over privacy and fraud on domestic platforms and to gain greater access to the global cybercrime market.

Background — The Chinese-Language Dark Web

Due to the distinct socio-political characteristics of China, the Chinese cybercrime landscape is unique in many ways. First, the online population of China is more than 2.5 times the population of the US, which provides a vast attack surface for cybercriminals. Second, due to the Great Firewall's sophisticated system of blocks and deterrents, Chinese internet users do not have access to some of the world's most visited websites. Instead, most blocked websites such as Facebook, Twitter, and YouTube have their homegrown equivalents to meet domestic demand and regulation requirements.



WEST	CHINA
f	Tencent 腾讯
amazon.com	阿里巴巴 Alibaba.com JD.京东 COM Tencent is top shareholder of JD.com
Google	Bai du 百度
NETFLIX	iQIYI 爱奇艺 腾讯视频 V.QQ.COM YOUKU 优酷 Baidu owns iQuiyi, Alibaba owns Youku, Tencent owns QQ video
	新浪微博 weibo.com Alibaba has 31.5% stake
UBER	滴滴 滴滴一下 美好出行
Spotify	阿里音乐 QQ音乐 Alibaba owns Ali music, Tencent owns QQ music, NetEase - China's fifth biggest internet company - owns NetEase Cloud Music
Expedia	Ctrip 途牛 tuniu.com 飞猪 Baidu is top shareholder od Ctrip, JD.com is top 2 shreholder of tuniu.com, Alibaba owns Fliggy

Figure 1: The Chinese counterparts of popular Western websites (Source: IMD)

China first gained worldwide web access in 1994, and it quickly became apparent to both early Chinese netizens and the government that the free flow of information could have serious political implications. By 1996, the Chinese government had already started taking steps to control the internet. Although the Great Firewall of China, as it exists today, is not the work of any one person in particular, Fan Binxing, a former computer science professor at the Harbin Institute of Technology, is widely regarded as the "Father of the Great Firewall", as he became the chief designer of the Great Firewall project in 1998. Some of the techniques employed by the Great Firewall include blocking IP addresses, DNS manipulations, and filtering specific URLs and keywords within URLs[1]. In research conducted by a team of academics from 4 US and Canadian universities from April to December 2020, it was found that the Great Firewall blocked around 311,000 domains. 41,000 of those were blocked by accident.

Chinese internet users are subject to some of the heaviest surveillance and censorship in the world. Under the direction of the 13th "Five Year Plan", covering 2016 to 2020, in which the government sought to strengthen information security and "step up" to take action against "subversion" in the struggle against "hostile" forces concerning cybersecurity sovereignty, the Chinese government carried out a series of 净网行动, or "Net Cleanup Activities" in 2019 and 2020. The activity in 2020 alone resulted in 1,522 individuals convicted for cybercrime[2]. In addition, 6,329 suspects were allegedly arrested in connection with online fraud related to the COVID-19 pandemic[3].

In light of these challenges, Chinese cybercriminals must operate with extra caution to conceal their identities and be highly adaptable at evading censorship and coping with sophisticated government surveillance and crackdowns. Like many other cybercrime ecosystems around the world, the Chinese cybercriminal underground consists of the familiar components of dark web and clearnet forums and marketplaces, instant messaging services, as well as threat actors crossing over into established international forums. Our research focuses on several specific dark web marketplaces in the Chinese underground but will also touch upon others as they are closely intertwined to form a complete underground ecosystem.

[1] The story of China's Great Firewall, the world's most sophisticated censorship system hxxps://www.scmp[.]com/abacus/who-what/what/article/3089836/story-chinas-great-firewall-worlds-most-sophisticated

[2] Ministry of Public Security: The Continuous Fight Against Cybercriminal Activities http://news.sina[.]com[.]cn/sf/news/fzrd/2020-04-16/doc-iirczymi6585012.shtml

[3] China toughens crackdown on cybercrime hxxp://www.china[.]org[.]cn/china/2020-04/11/content_75920202.htm

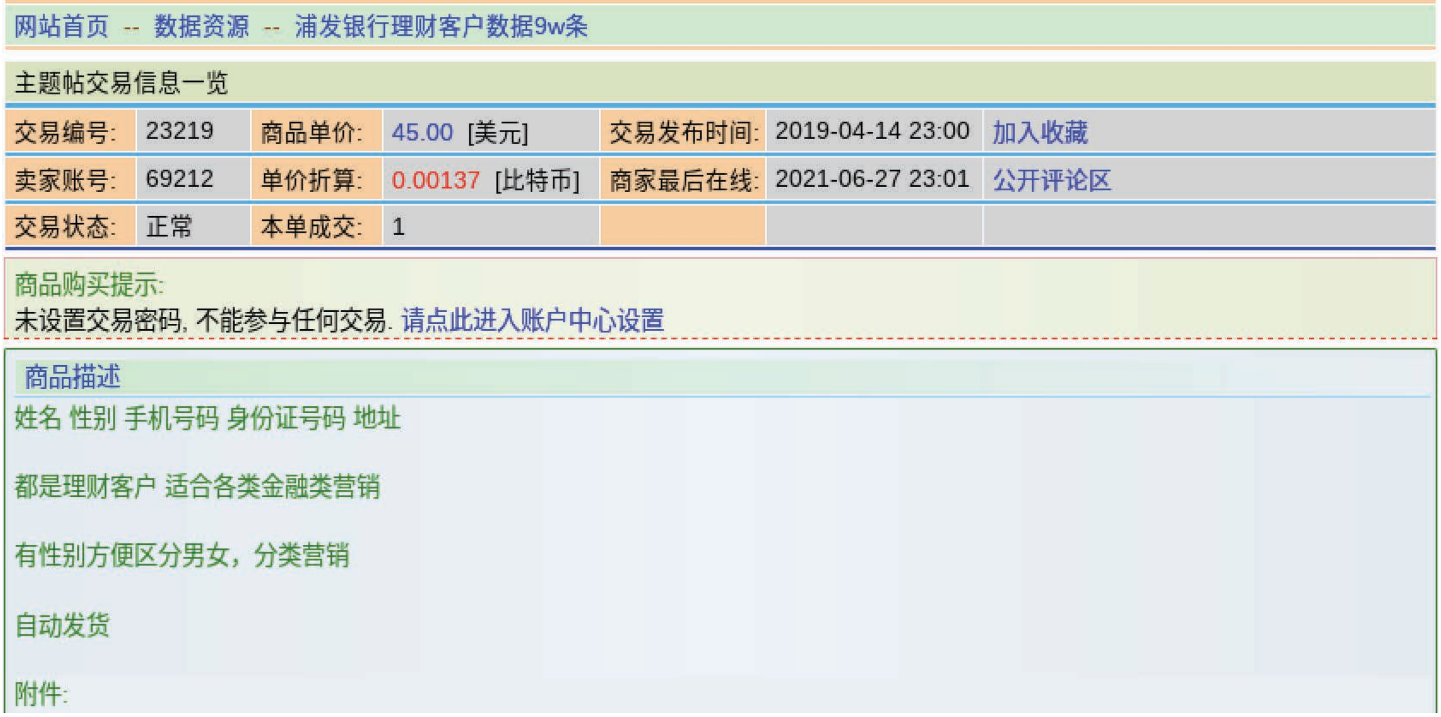
Major Dark Web Marketplaces

Since the objective of the Tor network is to protect anonymity, it is unsurprisingly blocked by the Great Firewall of China. Despite this, over 2,000 users connect to Tor from China each day through the official Tor infrastructure, and an unknown number use pre-proxies to connect and appear to be located outside of China.

We identified 8 major dark web marketplaces in the Chinese underground. They mostly cater to Chinese-speaking members on the dark web; only the Ali Marketplace (English and Chinese) and FreeCity Market (English, Chinese, and Korean) have other language options. The most popular offerings include stolen data, cybercrime tutorials, illicit services, physical goods, and pornography. Bitcoin is often the only accepted currency. Some of those marketplaces have withstood alleged distributed denial-of-service (DDoS) attacks and other service disruptions and have re-emerged, while others have disappeared over time, creating the suspicion of exit scams where website operators potentially stole the BTC wallets of registered members and vanished. Such speculations fueled a general lack of trust in the Chinese-language cybercriminal underground.

Exchange Market (交易市场)

The Exchange Market is the longest-running dark web marketplace in the Chinese underground. Its predecessor, the ChineseDeepWeb forum, was established in 2013. In 2015, due to the alleged DDoS attacks from unidentified state-sponsored threat actors, the website's administrator claimed it was necessary to implement server upgrade and escrow service to cover the expense of running the platform. Meanwhile, the website transitioned from a forum into a marketplace known as the DeepMix market and accepted bitcoins as the only form of payment. In fall 2019, DeepMix market once again came under prolonged DDoS attack and went offline. The marketplace resurfaced in December 2019 under the new name Exchange Market and appeared very similar to the original. It took several days for the website to recover most of its earlier posts. However, all the original threat actor handles were assigned a short numeric designator. Features such as seller ratings and reviews were also deleted, and newly registered handles are also limited to numeric designators only. The website's administrator claimed it is necessary to have many URLs and jump servers available to thwart potential DDoS attacks and to maintain the marketplace's availability. Although many other products and services are offered, Exchange Market is primarily known for its data offerings. Below is a typical offering from the Exchange Market, including customer data from the Shanghai Pudong Development Bank by threat actor "69212".



网站首页 -- 数据资源 -- 浦发银行理财客户数据9w条

主题帖交易信息一览

交易编号:	23219	商品单价:	45.00 [美元]	交易发布时间:	2019-04-14 23:00	加入收藏
卖家账号:	69212	单价折算:	0.00137 [比特币]	商家最后在线:	2021-06-27 23:01	公开评论区
交易状态:	正常	本单成交:	1			

商品购买提示:
未设置交易密码, 不能参与任何交易. 请点此进入账户中心设置

商品描述

姓名 性别 手机号码 身份证号码 地址

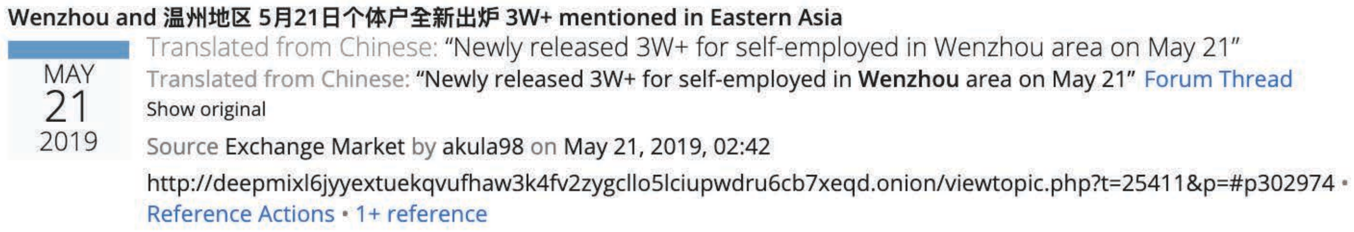
都是理财客户 适合各类金融类营销

有性别方便区分男女，分类营销

自动发货

附件:

Figure 2: An example posting from Exchange Market where the seller 69212 offered 90,000 records of financial management customers of Shanghai Pudong Development Bank. The heading displays the transaction number, seller account number, transaction status, unit price in dollars and BTC, number of successful transactions, the time the post was published, and the last time the seller was online. The item description indicates the data package contains the names, gender, cell phone numbers, personal ID numbers, and physical addresses of account holders. The seller also indicates that the data is from financial management customers and are categorized by gender for financial service type of marketing. The data will be sent automatically to buyers who have paid. (Source: Recorded Future)



Wenzhou and 温州地区 5月21日个体户全新出炉 3W+ mentioned in Eastern Asia

MAY 21 2019

Translated from Chinese: "Newly released 3W+ for self-employed in Wenzhou area on May 21"

Translated from Chinese: "Newly released 3W+ for self-employed in Wenzhou area on May 21" Forum Thread

Show original

Source Exchange Market by akula98 on May 21, 2019, 02:42

http://deepmixl6jyyextuekqvufhaw3k4fv2zygcllo5lciupwdru6cb7xeqd.onion/viewtopic.php?t=25411&p=#p302974 •

Reference Actions • 1+ reference

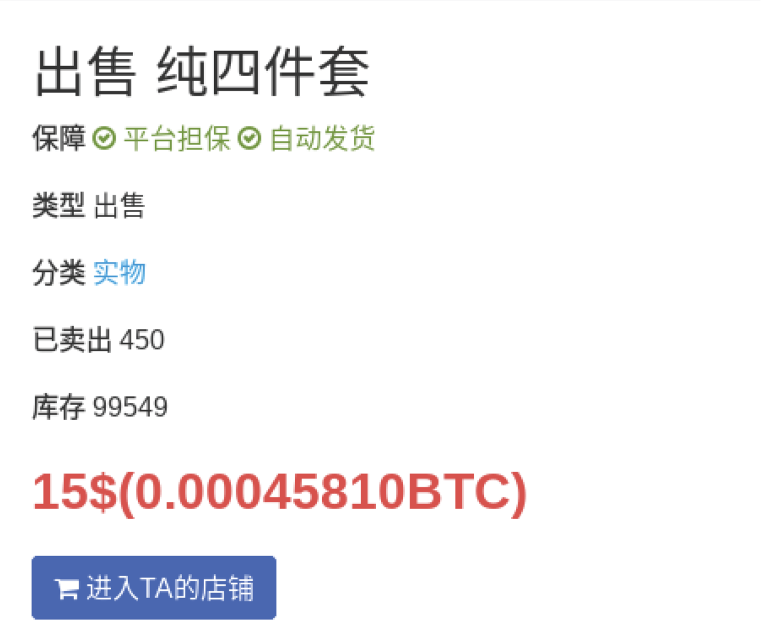
Figure 3: An offer from akula98 containing more than 30,000 records of self-employed small business owners from the Wenzhou area. (Source: Recorded Future)

On May 11, 2020, multiple Chinese media outlets reported the arrest of 27 suspects involved in cybercrimes. One of those arrested was a suspect with the online handle "akula98", who offered PII for sale on an undisclosed underground trading platform[4]. Research revealed that akula98 was active on the original DeepMix market and was primarily involved in selling leaked data. Below is a posting from akula98 on May 21, 2019 which advertised more than 30,000 records of self-employed small business owners of the Wenzhou area.

Tea Horse Road Market (茶马古道)

Tea Horse Road Market is a Chinese-language dark web marketplace that launched around April 2020. To register on the website, users need to provide a username, password, wallet password, and nickname. A registered account can be activated with $10 worth of bitcoins to access and post on the forum. The website consists of a marketplace, a forum, and a page for filing complaints against sellers. Near the top of the page is an advertisement section that includes items for sale, listed in USD and BTC, as well as items sought by buyers. A buyer needs to enter the wallet ID to purchase the item. For items that are wanted by a poster, a seller can contact the poster if they have a matching product to sell.

The official Telegram channel of Tea Horse Road is @tea_horsebot, although comments on the forum suggest that the account was closed a few months ago. There is a marketplace supervisor (市场监督员) who serves as the website administrator. Although the website claims to prohibit out-of-marketplace communications and transactions, many postings include Telegram, email, and other points of contact used by vendors. In addition, there are several unofficial Telegram channels which list marketplace offerings and announcements. Below is an offering of a set of 4 IDs for bank access posted on the marketplace.



出售 纯四件套

保障 ✓ 平台担保 ✓ 自动发货

类型 出售

分类 实物

已卖出 450

库存 99549

15$(0.00045810BTC)

Figure 4: An example posting from the Tea Horse Road Market where the seller is posting sets of 4 IDs for accessing Chinese bank accounts, which include personal IDs, bank cards, SIM cards, and the bank USB shield. The posting indicates the items are guaranteed by the platform and will be shipped automatically. It also shows that 450 items have been sold and 99,549 items remain in the inventory. The item is listed in both USD and BTC. By clicking on the blue bar, a visitor can view other items for sale by the seller. (Source: Recorded Future)

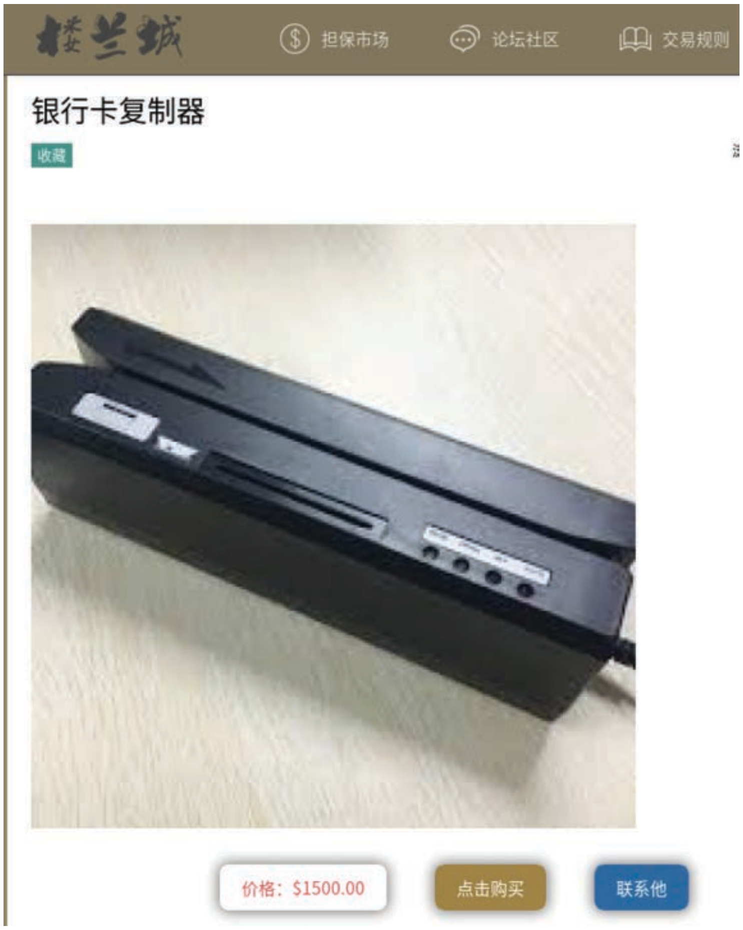
Loulan City Market (楼兰城)

Loulan City Market is a Chinese-language dark web marketplace and forum that started around April 2020. To register on the website, users need to provide a username, password, wallet password, and nickname. Loulan City Market has a Telegram channel, @awllc888, with more than 12,000 members, and the marketplace administrator ("管理员") makes public service announcements on the website.

Goods and services are divided into categories for leaked data, virtual goods, physical goods, services, pornography, and more. Postings in the marketplace are listed in USD, but BTC is the only accepted currency for transactions. A for-sale listing has information including the number of views and sales and also includes the handle of the seller's shop, seller's nickname, reputation score, and the number of items sold in the past 30

[4] Using "dark web" to sell 3.5 million records of data to promote POS, agent from Jiangsu arrested hxxps://www.sohu[.]com/a/397825155_135032

days. A buyer also has the option to contact the seller and view other items in the seller's shop. Below is an offering of an alleged bank card replicator (which resembles an MSR-206 magnetic stripe reader) for sale on the Loulan City Market by the threat actor "pangde".


楼兰城 担保市场 论坛社区 交易规则

银行卡复制器

收藏

价格：$1500.00 点击购买 联系他

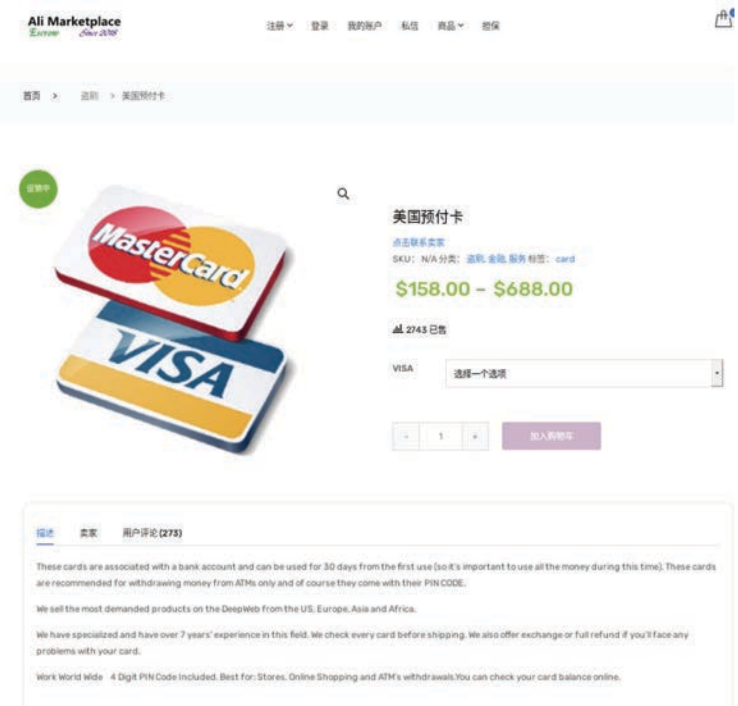
Figure 5: An alleged bank card replicator for sale on the Loulan City Market for $1,500. The brown button reads "click to buy" and the blue button reads "contact seller". (Source: Recorded Future)

Ali Marketplace

Ali Marketplace is an English- and Chinese-language dark web marketplace that launched in 2018. The marketplace does not require login credentials for browsing; however, registration with username, password, and email is required for conducting transactions. English is the default language of the website, but a user can switch the language to simplified Chinese, with Chinese-language content mostly being limited to headers and product listings. Its setup resembles some of the more established English and Russian language marketplaces rather than its Chinese-language counterparts, as it has a relatively stable lineup of "shops" running under a marketplace. At the time of this report, there were 20 standing advertisements listed by various threat actors, which included fraudulent account transfers, drugs, weapons, counterfeit documents and currencies, and credit card dumps.

Postings on the marketplace are listed in USD, but BTC is the only accepted currency for transactions. Individual product reviews on Ali Marketplace have been mostly positive. All purchases are handled through an escrow system. There is at least 1 moderator identified as "admin" who can be contacted through private messaging to resolve disputes and report rule violations.

While it is difficult to assess the origin of Ali Marketplace's operators, some signs might point to a collaborative effort between Chinese-speaking and international operators. In addition to its similarity to English or Russian-language marketplaces, the English language usage on the marketplace appears to be the work of non-native speakers. Below is a listing of alleged prepaid bank cards from the US in different denominations.


Ali Marketplace Escrow Since 2018

注册 登录 我的账户 私信 商品 担保

首页 > 盗刷 > 美国预付卡

促销中

美国预付卡

点击联系卖家

SKU：N/A 分类：盗刷, 金融, 服务 标签：card

$158.00 – $688.00

2743 已售

VISA 选择一个选项

- 1 + 加入购物车

描述 卖家 用户评论 (273)

These cards are associated with a bank account and can be used for 30 days from the first use (so it's important to use all the money during this time). These cards are recommended for withdrawing money from ATMs only and of course they come with their PIN CODE.

We sell the most demanded products on the DeepWeb from the US, Europe, Asia and Africa.

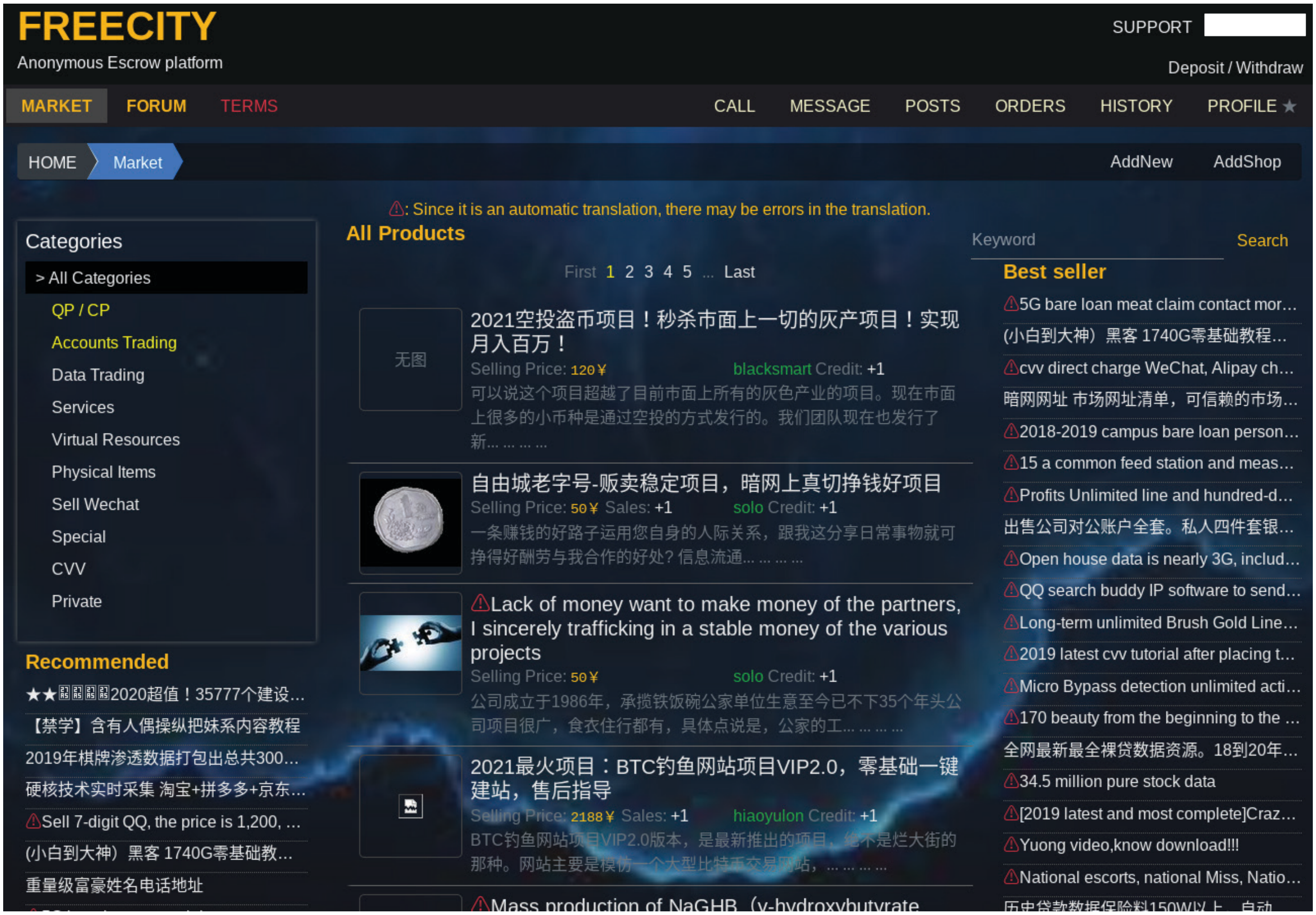
We have specialized and have over 7 years' experience in this field. We check every card before shipping. We also offer exchange or full refund if you'll face any problems with your card.

Work World Wide 4 Digit PIN Code included. Best for: Stores, Online Shopping and ATM's withdrawals.You can check your card balance online.

Figure 6: A listing of prepaid bank cards from the US. A buyer has the option to choose card balances from $158 to $688. The item description indicates that the cards are associated with a bank account and can be used for 30 days from the first use. The website's statistics indicate that 2,743 items have been sold, and there are 273 buyer reviews. (Source: Recorded Future)

FreeCity Market

FreeCity Market is an English-, Chinese-, and Korean-language dark web marketplace that advertises an array of products and services under the following categories: compromised data and accounts, services, physical and virtual commodities, WeChat data, and payment cards. Acceptable forms of payment include BTC, Ethereum (ETH), USD, and Chinese yuan (CNY). The leadership of the marketplace is unknown, but they operate at least 4 Telegram handles for communication and marketplace announcements: @freecitysocial, @freecitynews, @freecityadmin, and @freecityescrow.



⚠: Since it is an automatic translation, there may be errors in the translation.

Categories

- > All Categories
- QP / CP
- Accounts Trading
- Data Trading
- Services
- Virtual Resources
- Physical Items
- Sell Wechat
- Special
- CVV
- Private

Recommended

- ★★□□□□2020超值！35777个建设...
- 【禁学】含有人偶操纵把妹系内容教程
- 2019年棋牌渗透数据打包出总共300...
- 硬核技术实时采集 淘宝+拼多多+京东...
- ⚠Sell 7-digit QQ, the price is 1,200, ...
- (小白到大神）黑客 1740G零基础教...
- 重量级富豪姓名电话地址

All Products

2021空投盗币项目！秒杀市面上一切的灰产项目！实现月入百万！
Selling Price: 120￥ blacksmart Credit: +1
可以说这个项目超越了目前市面上所有的灰色产业的项目。现在市面上很多的小币种是通过空投的方式发行的。我们团队现在也发行了新... ... ...

自由城老字号-贩卖稳定项目，暗网上真切挣钱好项目
Selling Price: 50￥ Sales: +1 solo Credit: +1
一条赚钱的好路子运用您自身的人际关系，跟我这分享日常事物就可挣得好酬劳与我合作的好处？信息流通... ... ...

⚠Lack of money want to make money of the partners, I sincerely trafficking in a stable money of the various projects
Selling Price: 50￥ solo Credit: +1
公司成立于1986年，承揽铁饭碗公家单位生意至今已不下35个年头公司项目很广，食衣住行都有，具体点说是，公家的工... ... ...

2021最火项目：BTC钓鱼网站项目VIP2.0，零基础一键建站，售后指导
Selling Price: 2188￥ Sales: +1 hiaoyulon Credit: +1
BTC钓鱼网站项目VIP2.0版本，是最新推出的项目，绝不是烂大街的那种。网站主要是模仿一个大型比特币交易网站，... ... ...

⚠Mass production of NaGHB（γ-hydroxybutyrate

Best seller

- ⚠5G bare loan meat claim contact mor...
- (小白到大神）黑客 1740G零基础教程...
- ⚠cvv direct charge WeChat, Alipay ch...
- 暗网网址 市场网址清单，可信赖的市场...
- ⚠2018-2019 campus bare loan person...
- ⚠15 a common feed station and meas...
- ⚠Profits Unlimited line and hundred-d...
- 出售公司对公账户全套。私人四件套银...
- ⚠Open house data is nearly 3G, includ...
- ⚠QQ search buddy IP software to send...
- ⚠Long-term unlimited Brush Gold Line...
- ⚠2019 latest cvv tutorial after placing t...
- ⚠Micro Bypass detection unlimited acti...
- ⚠170 beauty from the beginning to the ...
- 全网最新最全裸贷数据资源。18到20年...
- ⚠34.5 million pure stock data
- ⚠[2019 latest and most complete]Craz...
- ⚠Yuong video,know download!!!
- ⚠National escorts, national Miss, Natio...
- 历史贷款数据保险料150W以上，自动

Figure 7: The landing page of the FreeCity Market with categories of offering and recommended listings to the left, a list of all products in the middle, and best sellers to the right. (Source: Recorded Future)

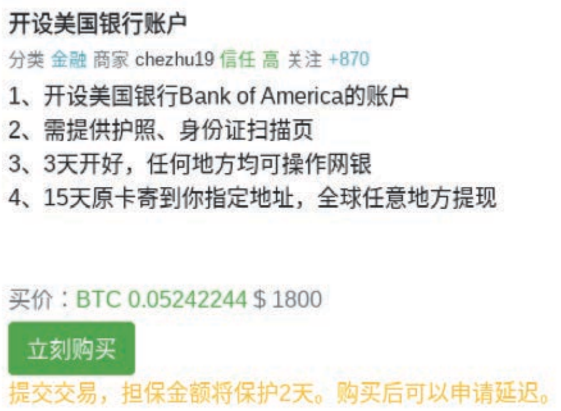
To register on the marketplace, a user is instructed to contact the Telegram handle @freecitysocial where they will receive a user ID and password. Once logged in, a user can update their profile information and must make a minimum $15 USD deposit to activate the account. Until a user makes the aforementioned deposit, a user can only view products and forum posts, but cannot purchase or participate.

FreeCity also operates a forum that is accessible on the marketplace's landing web page and includes the following forum thread topics: Darknet News, Crypto News, Hacking, Wuhan News, Free Group, Developer, Google Drive, and Free Resources. Forum users are instructed to only conduct deals, post advertisements, negotiate, or provide additional contact information through the marketplace.

Alibaba Market

Alibaba Market is a Chinese-language marketplace and forum that is only accessible via the Tor network. The website likely began operations in late-December 2019. To register an account, a user needs to provide a username, password, and $20 USD in BTC. A newly registered member is defaulted to a "medium" trust level, and a personal link is provided to each new member, which can be used to invite other members to join; the user will receive a 2% commission for each successful transaction of the invitee. There is also a link at the bottom of the homepage to contact the website administrator.

The postings are listed in BTC and USD. After the buyer initiates a transaction, the escrow amount will be protected for 2 days, and the duration can be extended upon request. The listing of items for sale is free; however, it is unknown how much commission the seller has to pay for successful transactions. Below is a screenshot of a listing by threat actor "chezhu19" which offers the service of opening a Bank of America account.



开设美国银行账户

分类 金融 商家 chezhu19 信任 高 关注 +870

1、开设美国银行Bank of America的账户
2、需提供护照、身份证扫描页
3、3天开好，任何地方均可操作网银
4、15天原卡寄到你指定地址，全球任意地方提现

买价：BTC 0.05242244 $ 1800

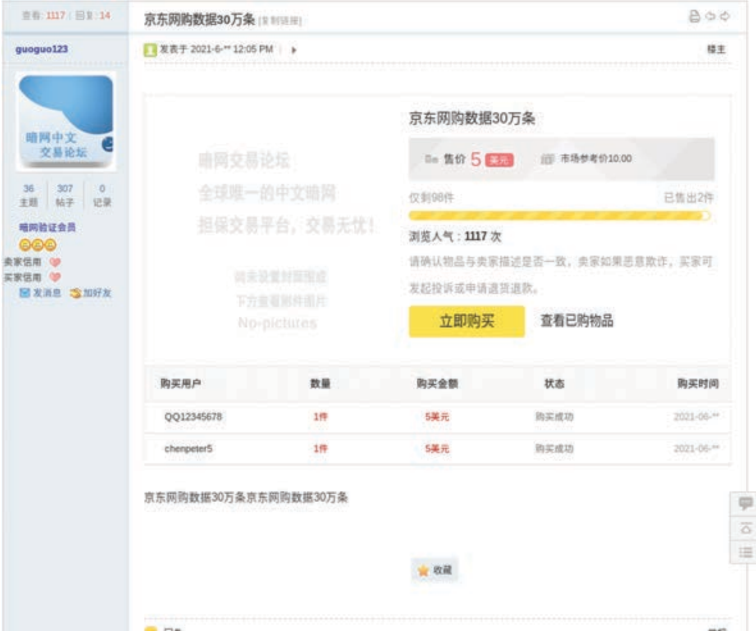
提交交易，担保金额将保护2天。购买后可以申请延迟。

Figure 8: A sample offer from the Alibaba Market where the seller chezhu19, who has a high trust level, is offering to open Bank of America accounts for fraudulent transactions. The buyer must provide a scanned passport or personal ID. The account will be set up in 3 days and the bank cards will be sent out to a designated address in 15 days, which can be used to withdraw cash from anywhere in the world. (Source: Recorded Future)

Dark Web Exchange (暗網中文交易論壇)

Dark Web Exchange is a Chinese-language marketplace and forum that is only accessible via the Tor network. Although the website's footer claims it has been in operation since 2001, the earliest posts are dated from November 2019. To register on the website, users need to provide a username, password, wallet password, and nickname. The postings are divided into data, carding, physical items, IDs, services, pornography, and more. The handle "暗网客服" (Dark Web Customer Service) acts as the website's administrator and makes public service announcements.

Below is the screenshot of a listing by the threat actor "guoguo123" which offered retail data from jd[.]com, a major Chinese online retailer.



京东网购数据30万条

售价 5 美元 市场参考价10.00

仅剩98件 已售出2件

浏览人气：1117 次

请确认物品与卖家描述是否一致，卖家如果恶意欺诈，买家可发起投诉或申请退货退款。

购买用户	数量	购买金额	状态	购买时间
QQ12345678	1件	5美元	购买成功	2021-06-**
chenpeter5	1件	5美元	购买成功	2021-06-**

京东网购数据30万条京东网购数据30万条

Figure 9: A sample offer from the threat actor "guoguo123", a verified member of Dark Web Exchange. The posting is 300,000 records of shopping data from jd[.]com, a major online retailer based in China. The price for the data package is $5. It has been viewed 1,117 times and purchased twice. (Source: Recorded Future)

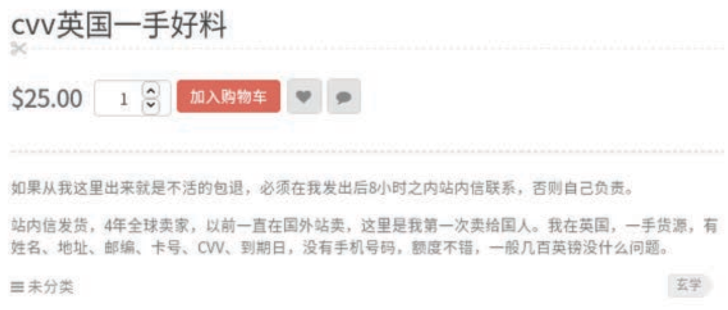
United Chinese Escrow Market (UCEM, 联合中文担保交易市场)

UCEM is a Chinese-language marketplace that opened on June 1, 2018, with a post from the administrator "admincn" to welcome shoppers. To register on the website, users need to provide a username, password, and an email address, although no login is required to browse the website. Unlike most dark web marketplaces, offerings on UCEM are relatively fixed and are organized in "stores" that are maintained by sellers. Some of the sample offerings include money laundering through account transfers, fraud tutorials, carding and hacking services, stolen data, and gift cards and card verification values (CVVs).

In addition to detailed product or service descriptions, each listing features buyer reviews, the number of items sold, and likes. Most buyer reviews appear to be positive. Postings in the marketplace are listed in USD, although all transactions are conducted with BTC. admincn posts periodic marketplace announcements and promotions on the landing page of the marketplace. The forum section mostly consists of questions and answers regarding transaction experiences.

The marketplace features a 15-day period escrow protection offered on all transactions without additional charge. The UCEM website homepage includes a section for buyers to discuss their transaction experiences, an internal mailbox function to communicate with other members, a BTC wallet management section, and an FAQ section that explains the rules of behavior on the marketplace. Like the Exchange Market, UCEM was also affected by DDoS attacks in the fall of 2019, but by late November 2019, the UCEM administrator announced that the forum was resuming operations.

Below is the screenshot of a listing by the threat actor "英国一手卡料出售CVV" (First-hand CVV carding material from UK), which are allegedly first-hand CVVs from U.K.



cvv英国一手好料

$25.00 1 加入购物车

如果从我这里出来就是不活的包退，必须在我发出后8小时之内站内信联系，否则自己负责。

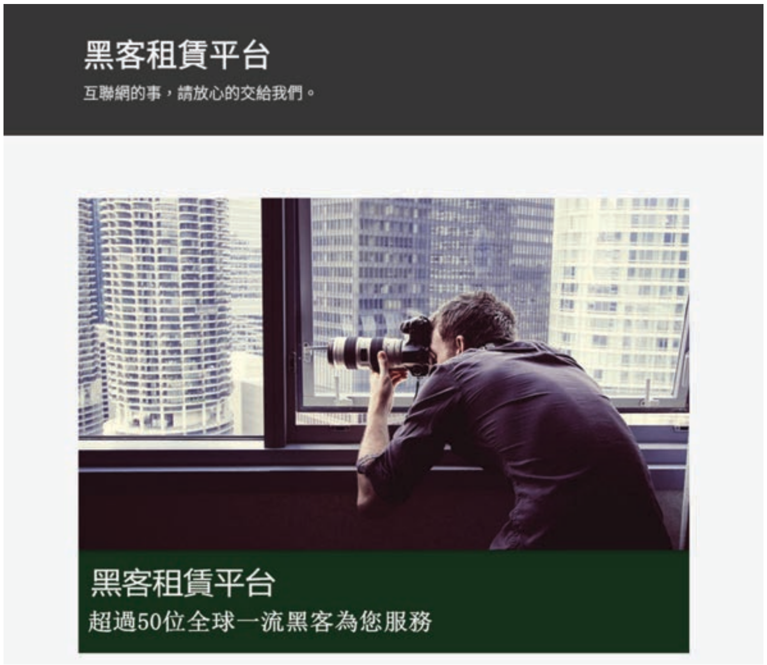
站内信发货，4年全球卖家，以前一直在国外站卖，这里是我第一次卖给国人。我在英国，一手货源，有姓名、地址、邮编、卡号、CVV、到期日，没有手机号码，额度不错，一般几百英镑没什么问题。

☰ 未分类 玄学

Figure 10: A sample listing on UCEM where credit cards from the United Kingdom are offered for $25 each. The seller guarantees the validity of credit card numbers and accepts returns if they are not, but the buyer must contact the seller within 8 hours after receipt. The seller claims to have sold credit card numbers worldwide for 4 years but says that this is their first time selling to Chinese customers. The seller also claims to be based in the UK and to have first-hand sources. The data includes names, addresses, postal codes, credit card numbers, CVVs, and expiration dates. (Source: Recorded Future)

Other Dark Web Markets

Besides the aforementioned websites, there are smaller and lower-tier shops that claim to perform hacking for hire, cryptocurrency trading, money laundering, and other illicit services. One such example is "黑客租赁平台" (Hacker for Hire Platform), the landing page of which is shown in Figure 11, below.



黑客租賃平台

互聯網的事，請放心的交給我們。

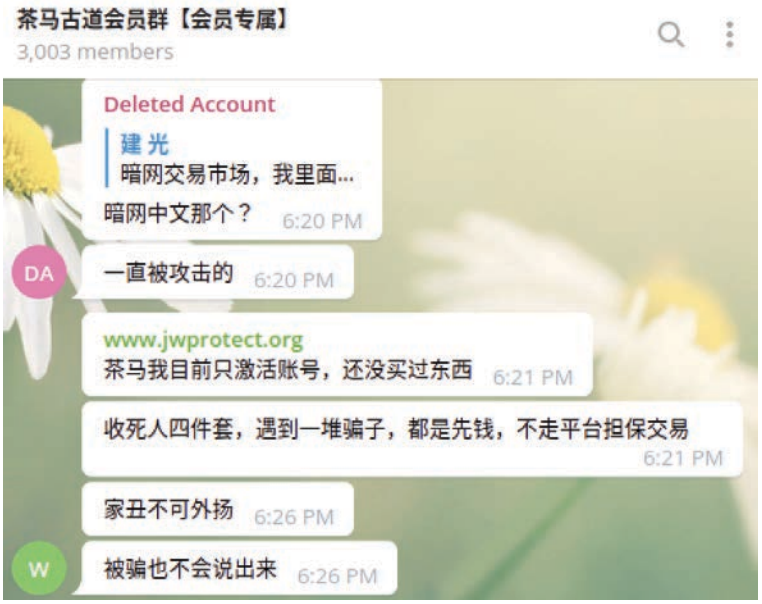
黑客租賃平台

超過50位全球一流黑客為您服務

Figure 11: The landing page of 黑客租赁平台, a Chinese-language dark web hacker-for-hire website, which claims to have over 50 world-class hackers in service. (Source: Recorded Future proprietary data)

Over time, some of the lower-tier dark web marketplaces have popped up and then disappeared. Some of these markets may have committed exit scams, while others may have been affected by their hosting providers. One market, Darkweb Chinese-Language Forum, had only existed for about a week before Daniel's Hosting was hacked on March 10, 2020. Daniel Winzen, the developer of the namesake hosting service, stated that an unknown attacker gained access to the backend and deleted its entire hosting database, which caused 7,600 dark web portals to go offline. The layout of Darkweb Chinese-Language Forum was nearly identical with Coinmixex and ChinaDarkweb, 2 older Chinese language cybercriminal forums that are also now defunct. They were all PHP-based and possibly hosted by Daniel's hosting as well.

The frequent turnover and bad experiences on these dark web marketplaces are often discussed on Chinese-language Telegram channels and dark web directories, which fuels the general lack of trust of the Chinese cybercriminal underground. Below are a few examples of this sentiment.



茶马古道会员群【会员专属】
3,003 members

Deleted Account
建 光
暗网交易市场，我里面...
暗网中文那个？ 6:20 PM

DA 一直被攻击的 6:20 PM

www.jwprotect.org
茶马我目前只激活账号，还没买过东西 6:21 PM

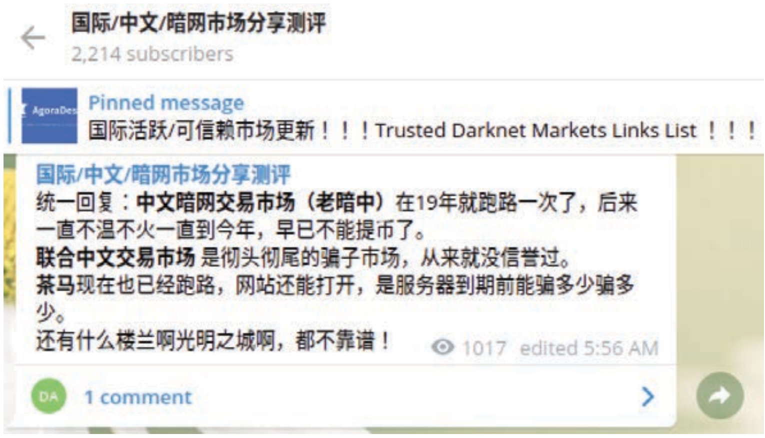
收死人四件套，遇到一堆骗子，都是先钱，不走平台担保交易 6:21 PM

家丑不可外扬 6:26 PM

W 被骗也不会说出来 6:26 PM

Translation of conversation:
[Replying to a comment on the Exchange Market from a Deleted Account] The old Chinese Dark Web?
DA: The one that's constantly under attack.
For Tea Horse Road I only have an activated account but have not bought anything yet.
They sell the sets of four IDs from dead people. I've run into a bunch of crooks, they always want money first and want to evade the platform's escrow. Family's dirty secret cannot be divulged.
W: Those who were cheated would not speak up.

Figure 12: Discussions about Exchange Market and Tea Horse Road Market on one of the Telegram channels for Tea Horse Road Market members. (Source: Recorded Future proprietary data)



国际/中文/暗网市场分享测评
2,214 subscribers

Pinned message
国际活跃/可信赖市场更新！！！Trusted Darknet Markets Links List！！！

国际/中文/暗网市场分享测评
统一回复：**中文暗网交易市场（老暗中）**在19年就跑路一次了，后来一直不温不火一直到今年，早已不能提币了。
联合中文交易市场 是彻头彻尾的骗子市场，从来就没信誉过。
茶马现在也已经跑路，网站还能打开，是服务器到期前能骗多少骗多少。
还有什么楼兰啊光明之城啊，都不靠谱！

1017 edited 5:56 AM

1 comment

Translation of posting::
International/Chinese/Dark Web Market Sharing and Assessment
Pinned message - Trusted Darknet Markets Links List!!!
International/Chinese/Dark Web Market Sharing and Assessment
Reply to all: The Exchange Market (Old Chinese Dark Web) had gone offline once in 2019, then it has been lukewarm ever since up to this year, and you can no longer withdraw bitcoin.
The United Chinese Escrow Market is a total fraud, it has never been reliable.
Tea Horse Road has also gone off the rails, you can still access the website, but the server is about to expire and it's trying to cheat as much as it can.
As for Loulan City, Light City, etc., none of them is reliable!

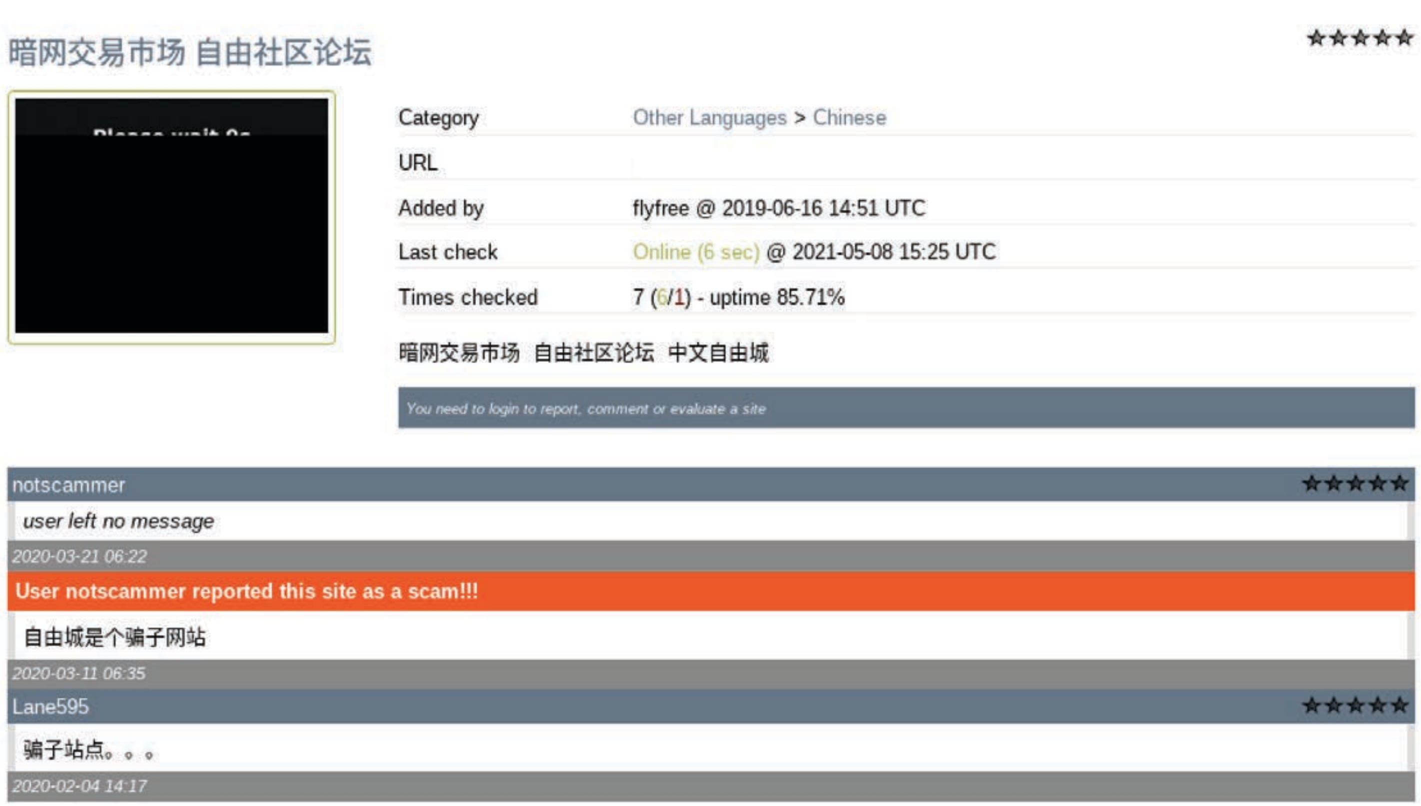
Figure 13: On a Telegram channel titled "International/Chinese/Dark Web Market Sharing and Assessment", a posting to all members exposed the fraudulent nature of several major Chinese-language dark web markets including the Exchange Market, United Chinese Escrow Market, Tea Horse Road Market, Loulan City Market, and Light City Market (a short-lived market that is now offline). (Source: Recorded Future proprietary data)

Characteristics of Offerings on Chinese Underground Marketplaces

Most Chinese-language dark web marketplaces are escrow markets where part or all of the payment is held until the goods or service purchased is delivered. The items are mostly listed in US dollars (USD); however, bitcoin (BTC) is often the only accepted currency. Our reseach across Chinese-language dark web sources found the following to be the the most popular offerings: leaked data, cybercrime tutorials, money laundering service, credit card dumps, pornography, physical goods, and malware. Meanwhile, items such as infostealer logs, as those advertised on Russian Market or Genesis Market, are not found in the Chinese underground.

Telegram channels, both official and unofficial, are often associated with dark web marketplaces. Although most dark web marketplaces prohibit communications outside the platform, sellers often post Telegram handles as contact information.

Below is a breakdown of some of the most popular offerings.



暗网交易市场 自由社区论坛

★★★★★

Category	Other Languages > Chinese
URL	
Added by	flyfree @ 2019-06-16 14:51 UTC
Last check	Online (6 sec) @ 2021-05-08 15:25 UTC
Times checked	7 (6/1) - uptime 85.71%

暗网交易市场 自由社区论坛 中文自由城

You need to login to report, comment or evaluate a site

notscammer ★★★★★
user left no message
2020-03-21 06:22

User notscammer reported this site as a scam!!!
自由城是个骗子网站
2020-03-11 06:35

Lane595 ★★★★★
骗子站点。。。
2020-02-04 14:17

Figure 14: Entry for Free City Market on a dark web directory. Both users indicated that Free City Market is a fraudulent website. (Source: Recorded Future proprietary data)

Compromised Data: PII From Different Platforms

Personally identifiable information (PII) can be found in a variety of compromised data sets. In addition to the obvious sources such as consumer data from financial service companies and business directories, they can also be found in exfiltrated data from illegal gambling apps and loan apps, which are unique to China. The stolen PII can be monetized and used by cybercriminals to engage in social engineering and credential stuffing attacks. The section below examines some of the most popular forms of compromised data offered on the Chinese-language dark web markets.

Some examples of data offerings include consumer PIIs from large banks and insurance companies based in China. For instance, the data from various subsidiaries of Ping An Insurance (Group) Co. Ltd., one of the largest financial conglomerates of China, is frequently offered in various dark web marketplaces.

Source	Event
Tea Horse Road Market	On June 5, 2021, more than 130,000 records of nationwide loan data from Ping An Bank from May 12, 2021 were offered by the actor “475154” for $16. The data includes names of branch offices, names of customers, loan balances, types of customers, types of loans, and cell phone numbers.
Loulan City Market	On May 27, 2021, 730,000 records of nationwide insurance data from Ping An Insurance from 2020 were offered by the actor “Quanshao” for $48. The data includes product types, balances, duration of insurance, names, personal ID numbers, genders, cell phone numbers, emails, provinces, cities, monthly incomes, marital status, types of insurance, insurance liabilities, insurance objectives, and premium due dates.
Exchange Market	On May 9, 2021, a private transaction of 500 records of customer contracts from Ping An Insurance for $50 was conducted between undisclosed parties on the market.
FreeCity Market	On March 9, 2021, 32 million records of nationwide insurance data from Ping An Insurance, which can be ordered based on province, were offered by an anonymous seller.

Another popular type offering is PII information of business owners:

Source	Event
Dark Web Exchange	On June 10, 2021, a posting of an internal government directory containing business owner data, including cell phone numbers, was offered by the threat actor “m12345666” for $294.
Tea Horse Road Market	On June 3, 2021, 190,000 records of business owner data from Guangzhou were offered by the threat actor “396767” for $10. The data includes company names, names of persons in charge, registration addresses, and associated bank account numbers.
Loulan City Market	On June 3, 2021, 90,000 records of female business owners nationwide were offered by the threat actor “wlwjgswd” for $20. The data includes names, membership associations, philanthropy indexes of corporations, popularity indexes, and activity levels.

Data offering on Chinese-language dark web marketplaces is not limited to Chinese sources. International consumer data sets, such as those from India, South Korea, US, and Canada, are often found on these dark web marketplaces as well:

Source	Event
Exchange Market	On June 10, 2021, more than 10,000 records of Chinese Canadian citizens were offered by the threat actor “646464” for $1,550. It is not clear from the post whether the information was obtained from Chinese or Canadian sources.
Tea Horse Road Market	On June 8, 2021, more than 1 million records of customer information, including PII and credit card numbers from the South Korean web portal www.nate[.]com, were offered by the threat actor 476577 for $299.
Loulan City Market	On May 22, 2021, more than 575,00 records of shareholder data from India were offered by the threat actor “pdfkfg” for $150. The data includes names, emails, cell phone numbers, occupations, and the addresses of shareholders.

Gambling data is very popular on Chinese-language dark web marketplaces due to the unique environment and laws of China. All forms of gambling are outlawed in China, with state-run lottery the lone exception. The only legal casinos are located in Macau. Those who want to gamble in mainland China must turn to illegal channels. In response, the Chinese government has stepped up its effort to stop people from gambling, including using big data to crack down on cross-border gambling. In June 2020, the Chinese Ministry of Security launched an online website where people can report cross-border gambling instances[5].

[5] China Using Big Data to Prevent Citizens from Gambling Internationally hxxps://www.casino[.]org/news/china-using-big-data-to-prevent-citizens-from-gambling-internationally/

Based on law enforcement data, the surge in illegal online gambling amid the pandemic has been astonishing. By the end of September 2020, Chinese authorities launched investigations of more than 8,800 cross-border gambling cases and arrested more than 60,000 suspects allegedly involved in the illegal businesses[6]. The "Net Cleanup Activity" of 2021 makes the crackdown of illegal gaming a priority. The campaign is a multi-agency effort led by the National Office Against Pornography and Illegal Publications, launched on March 19, 2021[7].

Quite often, gambling platforms and apps are not designed with security in mind and are thus highly vulnerable. In addition, gambling data often include PII, which can be exploited by cybercriminals. Rival platform operators sometimes engage in hacking and DDoS operations to drive competitors out of business.

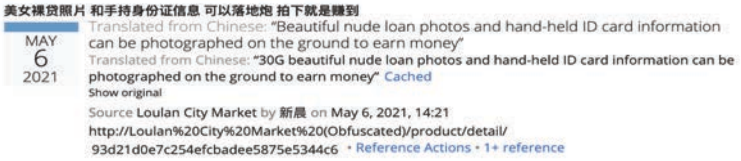
Below are examples of gambling data and tutorial offerings:

Source	Event
Tea Horse Road Market	On June 5, 2021, a posting of the source code and services required in building a gambling and gaming website was offered by the threat actor "476404" for $888.
Loulan City Market	On May 31, 2021, a posting of exfiltrated gambling and sports betting data was offered by the threat actor "路思蓉" (Lu Si Rong) for $190.00. The threat actor claimed the data was first-hand and different sizes of data packages are available.
Tea Horse Road Market	On Mar. 13, 2021, a posting of exfiltrated mobile gaming data was offered by the threat actor "427297" for $19. The data includes customer cell phone numbers, address data (provinces and cities), gaming platform operators, and URLs.

Another underground offer often related to online gambling is blackhat SEO, which are ways to improve search ranking by exploiting search engine guidelines. In Chinese, it is referred to as 引流, which means drawing traffic. Its tutorials are commonly offered on dark web marketplaces.

Source	Event
Tea Horse Road Market	On June 8, 2021, a posting which offered the scripts for drawing traffic for 17 mobile apps was offered by the threat actor "454770" for $10.
Loulan City Market	On May 17, 2021, a tutorial on how to draw traffic on TikTok was offered by the threat actor "jk1996" for $300.
Exchange Market	On Mar. 13, 2021, a tutorial on how to draw traffic and attract fans for QQ groups was offered by the actor "634642" on Exchange Market for $150.

Due to strict restrictions in China for business and student loans, black market mobile application-based money lenders seize the opportunity to launch peer-to-peer (P2P) loans with high interest rates. Lenders often coerce female borrowers into providing nude pictures and identifications as collateral and threaten to release them to the borrower's family or the public in case of missed payments. For male borrowers, the lenders subject the borrower's family and friends to threatening phone calls and text messages. Although the Chinese government launched a crackdown on illegal P2P loans in 2020, nude pictures associated with borrower's PII (known as "nude loan") are still frequently traded on dark web marketplaces. One such threat actor, named "新晨" (Xin Chen), offered nude loan photos of female borrowers holding personal IDs on Loulan City Market for $20.



美女裸贷照片 和手持身份证信息 可以落地炮 拍下就是赚到

MAY 6 2021

Translated from Chinese: "Beautiful nude loan photos and hand-held ID card information can be photographed on the ground to earn money"

Translated from Chinese: "30G beautiful nude loan photos and hand-held ID card information can be photographed on the ground to earn money" Cached

Show original

Source Loulan City Market by 新晨 on May 6, 2021, 14:21

http://Loulan%20City%20Market%20(Obfuscated)/product/detail/93d21d0e7c254efcbadee5875e5344c6 • Reference Actions • 1+ reference

Figure 15: An offer for nude photos of female loan borrowers with their ID cards posted on the Loulan City Market (Source: Recorded Future)

Due to the crackdown on P2P loans at home, Chinese cybercriminals have moved their operations to neighboring countries. As India entered lockdown due to the Covid-19 pandemic in 2020, loan operators started lending high-interest loans to businesses in need of cash. In January 2021, 2 Chinese nationals were arrested in Bengaluru, India for running illegal lending apps, collecting exorbitant interests, and threatening clients for missed payments. The police also arrested a few Indian nationals who operated a call center and assisted the Chinese nationals in debt collections[8].

[6] How China's E-Commerce Giants Enable Illegal Online Gambling hxxps://asia.nikkei[.]com/Spotlight/Caixin/How-China-s-e-commerce-giants-enable-illegal-online-gambling

[7] "Net Cleanup Campaign is Here": Crackdowns on Unlicensed Games, Banning the Streaming of Unapproved Games hxxps://new.qq[.]com/omn/20210319/20210319A0EUSJ00.html

[8] Deep Dive | How China-Based Money Lending Apps Are Devastating Gullible Indian Borrowers hxxps://www.indiatoday[.]in/india/story/deep-dive-how-china-based-money-lending-apps-devastating-gullible-indian-borrowers-1756569-2021-01-06

Money Laundering

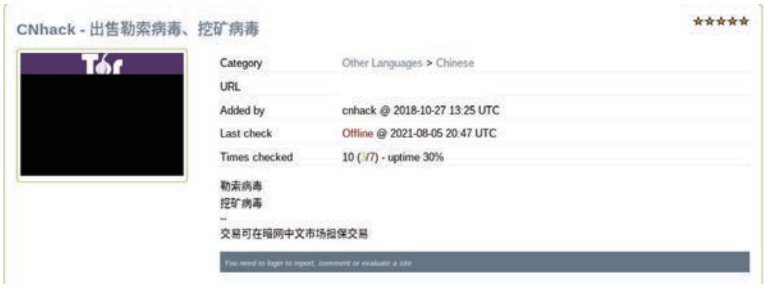
Money laundering services and tutorials are widely offered across different Chinese dark web marketplaces, and sometimes disguised as “cryptocurrency investment services”.

Source	Event
Tea Horse Road Market	On June 11, 2021, a tutorial on using BTC cryptocurrency for money laundering was offered by the actor “419972” for $2.
Exchange Market	On June 3, 2021, a tutorial on using Monero cryptocurrency for money laundering was offered by the actor “628526”.
United Chinese Escrow Market	On May 14, 2021, a group known as “国际洗钱公司” (International Money Laundering Company) advertised their service and set a deposit of $500.

At the time of this report, the Chinese government is stepping up on the crackdown of money laundering operations through cryptocurrency. In early June 2021, Operation Card Breaking campaign[9], which was the fifth round of the nationwide crackdown on money laundering activities, saw over 1,000 people arrested in China over charges of money laundering through crypto-currency. A Chinese-language dark web cryptocurrency investment website also went offline around the same time.

Malware

Malware is not a major component of Chinese-language dark web marketplaces. The offerings are mostly limited to basic items such as GSM sniffers and Android RATs. However, there have been a few malware related postings by more sophisticated malware threat actors. One such threat actor is cnhack, who was active on both DeepWebChinese and DeepMix, the previous incarnations of Exchange Market. The threat actor authored the custom FilesL0cker ransomware and sought affiliates on DeepWebChinese. However, the threat actor claimed that the latest version of the ransomware did not work as it would not decrypt files on an infected host even with the decryption key. The threat actor later claimed to have joined the GandCrab affiliate program and encouraged others to do so. cnhack operated a Tor website to sell ransomware and cryptominers, but the website’s URL no longer resolves.



CNhack - 出售勒索病毒、挖矿病毒

Category	Other Languages > Chinese
URL	
Added by	cnhack @ 2018-10-27 13:25 UTC
Last check	Offline @ 2021-08-05 20:47 UTC
Times checked	10 (3/7) - uptime 30%

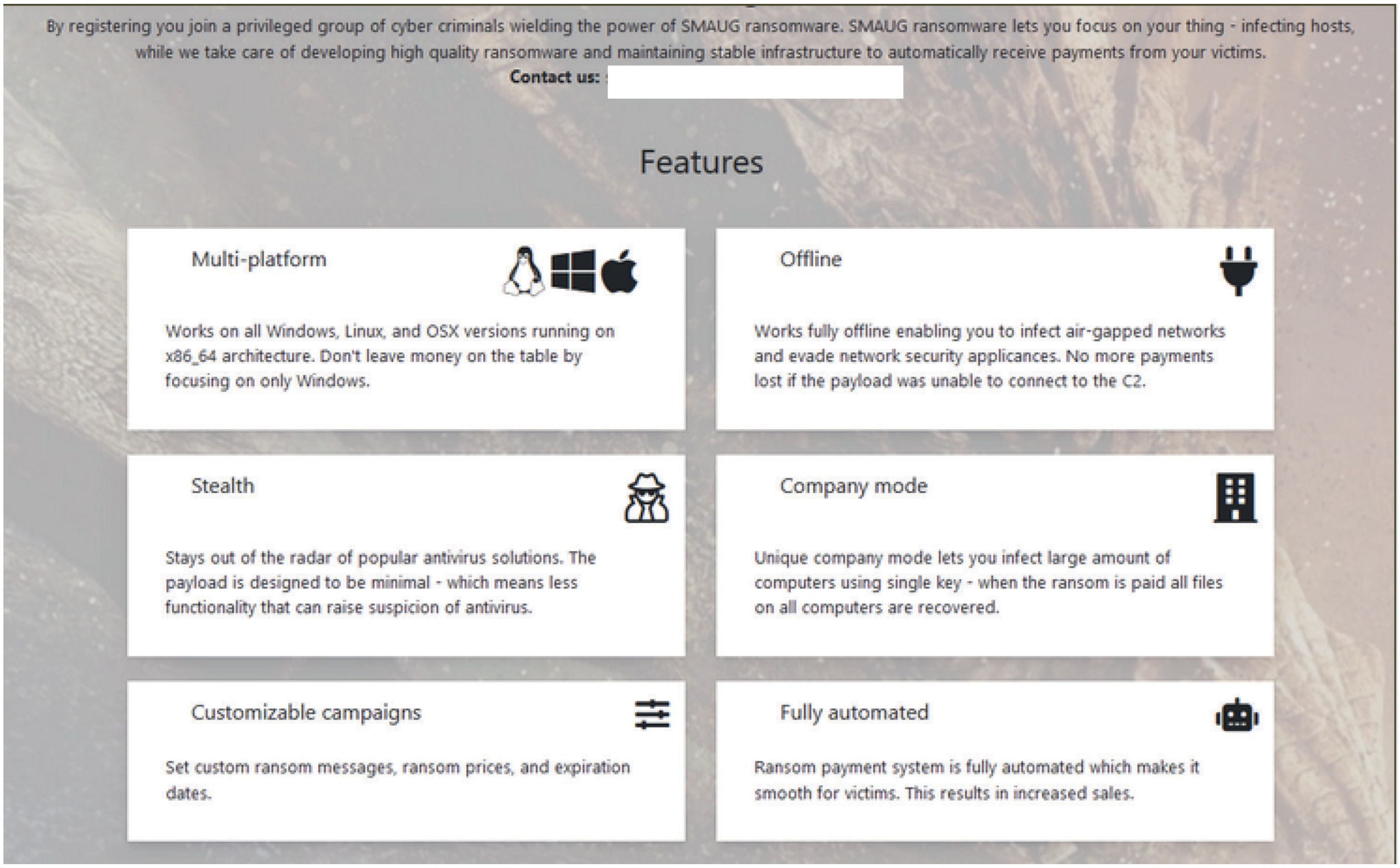
勒索病毒
挖矿病毒
--
交易可在暗网中文市场担保交易

You need to login to report, comment or evaluate a site

Figure 16: cnhack’s Tor website on a dark web directory, which indicated that the threat actor was advertising ransomware and cryptocurrency-mining malware and claimed that the transaction can be conducted on the Exchange Market. The directory indicates the website has been offline since as late as August 5, 2021 and the URL to the Tor site no longer resolves. (Source: Recorded Future proprietary data)

On May 6, 2020, the threat actor 556307 advertised the Smaug ransomware affiliate program on the Exchange Market. The threat actor claimed to have authored the ransomware, including the source code and a tutorial on how to run it. Below is a screenshot of the functions of the ransomware. The post also provided a Tor-based link for affiliate program registration, but the link no longer resolves. Below is a screenshot of the purported functions of the ransomware. There is a possibility that 556307 and cnhack could be the same person but since the latest incarnation of Exchange Marketarbitrarily assigned existing handles to numerical only handles, it is difficult to establish links between earlier and later posts.

[9] Chinese Police Arrest 1.1K People on Crypto-Related Money Laundering Charges hxxps://www.coindesk[.]com/chinese-police-arrest-1-1k-people-on-crypto-related-money-laundering-charges



By registering you join a privileged group of cyber criminals wielding the power of SMAUG ransomware. SMAUG ransomware lets you focus on your thing - infecting hosts, while we take care of developing high quality ransomware and maintaining stable infrastructure to automatically receive payments from your victims.

Contact us: [redacted]

Features

Multi-platform

Works on all Windows, Linux, and OSX versions running on x86_64 architecture. Don't leave money on the table by focusing on only Windows.

Offline

Works fully offline enabling you to infect air-gapped networks and evade network security applicances. No more payments lost if the payload was unable to connect to the C2.

Stealth

Stays out of the radar of popular antivirus solutions. The payload is designed to be minimal - which means less functionality that can raise suspicion of antivirus.

Company mode

Unique company mode lets you infect large amount of computers using single key - when the ransom is paid all files on all computers are recovered.

Customizable campaigns

Set custom ransom messages, ransom prices, and expiration dates.

Fully automated

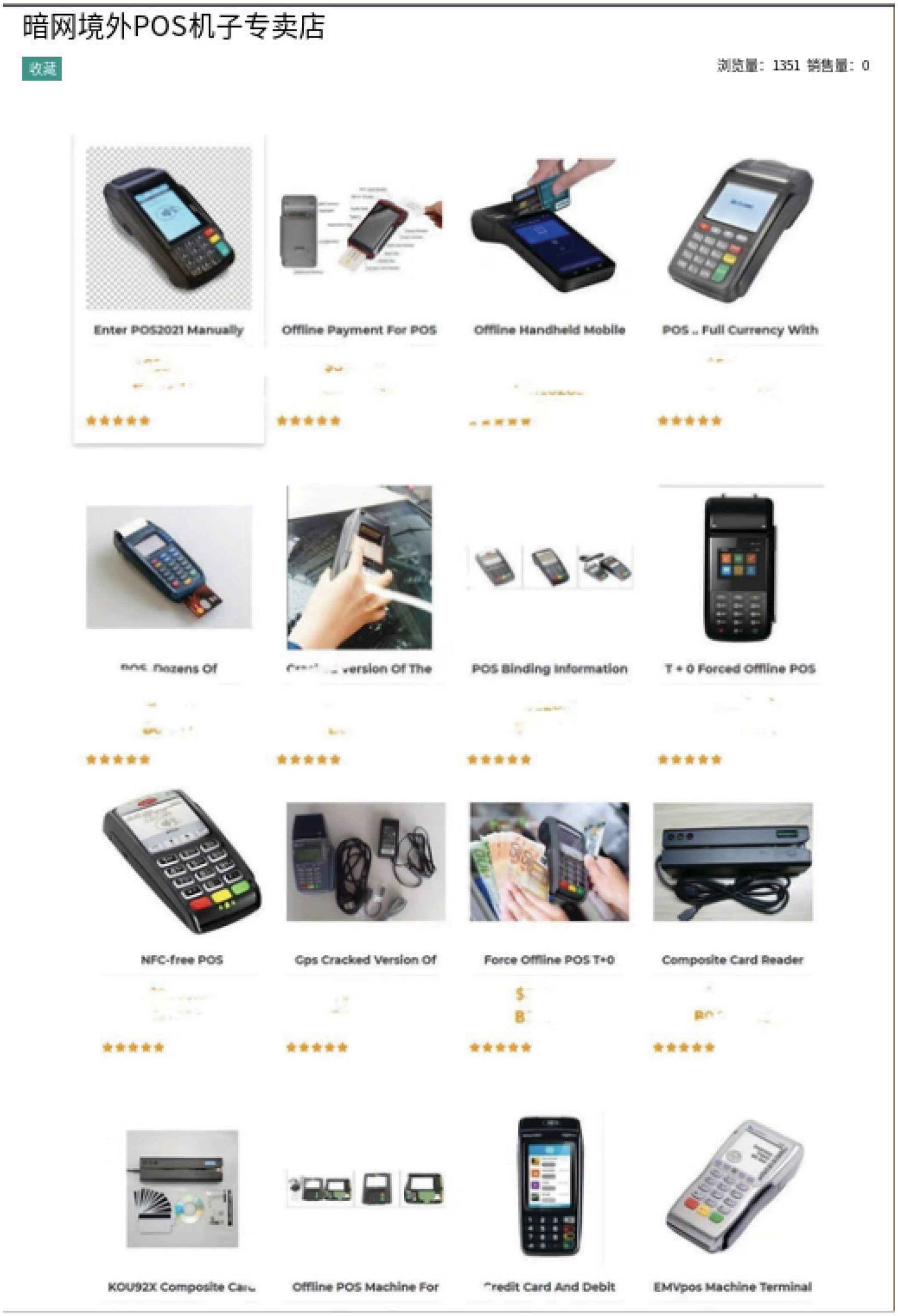
Ransom payment system is fully automated which makes it smooth for victims. This results in increased sales.

Figure 17: Description of the Smaug ransomware (Source: Recorded Future)

Physical Items

Due to the threat to anonymity, physical items are not as widely offered as data or other types of virtual goods, but are still part of the regular postings on Chinese-language dark web marketplaces. They often include the 4 identifications required to access Chinese bank accounts (personal IDs, SIM cards, bank cards, and bank USB shield), point-of-sale (POS) skimmers, weapons, counterfeit currency, and drugs.

Source	Event
Dark Web Exchange	On May 30, 2021, a posting of guns and ammunition manufacturing and shipping service was made by the threat actor “BMG”. The threat actor claimed to be based in Myanmar and have associates in Ukraine, and specialize in manufacturing high-fidelity replicas of various rifles and pistols.
Tea Horse Road	On May 17, 2021, a shipping service of allegedly high-quality cannabis was made by the threat actor “461747”.
Loulan City Market	On May 11, 2021, an advertisement of overseas POS skimmer shop was posted by the threat actor “境外 POS” (Overseas POS), where an assortment of credit card skimmers are offered for $3,000 each.
Exchange Market	Dec. 31, 2020, a service that offers high-fidelity counterfeit RMB in small denominations was posted by the actor “567430”.



暗网境外POS机子专卖店

收藏

浏览量：1351 销售量：0

Enter POS2021 Manually

Offline Payment For POS

Offline Handheld Mobile

POS .. Full Currency With

POS Dozens Of

Cracked version Of The

POS Binding Information

T + 0 Forced Offline POS

NFC-free POS

Gps Cracked Version Of

Force Offline POS T+0

Composite Card Reader

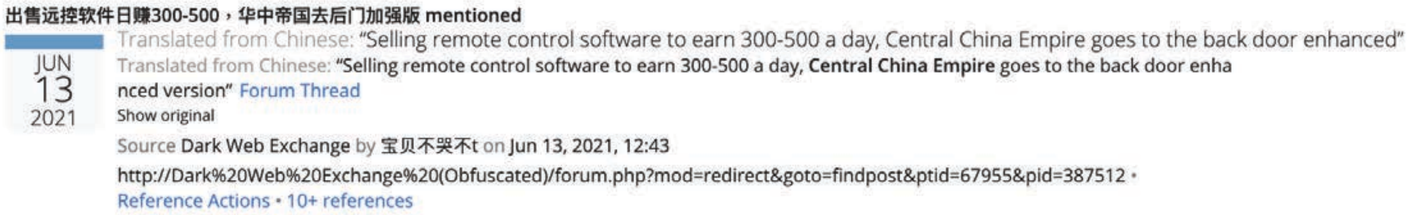
KOU92X Composite Card

Offline POS Machine For

Credit Card And Debit

EMVpos Machine Terminal

Figure 18: An advertisement by the threat actor "Overseas POS", who specializes in the sales of overseas point-of-sale skimmers for $3,000 each. (Source: Recorded Future)



出售远控软件日赚300-500，华中帝国去后门加强版 mentioned

JUN 13 2021

Translated from Chinese: “Selling remote control software to earn 300-500 a day, Central China Empire goes to the back door enhanced”

Translated from Chinese: “Selling remote control software to earn 300-500 a day, **Central China Empire** goes to the back door enha nced version” Forum Thread

Show original

Source Dark Web Exchange by 宝贝不哭不t on Jun 13, 2021, 12:43

http://Dark%20Web%20Exchange%20(Obfuscated)/forum.php?mod=redirect&goto=findpost&ptid=67955&pid=387512 •

Reference Actions • 10+ references

Figure 19: A RAT from the now-defunct Central China Empire Forum with an enhanced backdoor was offered on the Dark Web Exchange. (Source: Recorded Future)

Clearnet Hacking Forums and Blogs

The origin of China’s clearnet hacking forums dates back to the early 2000s. After the collision between the American EP-3 spy plane and a Chinese fighter jet near the Chinese island of Hainan, a weeklong “Cyber War” was declared between Chinese and American hackers in early May 2001, which led to the defacement of websites in both countries. The Honker Union of China was one of the leading groups that launched attacks on the Chinese side. After disbanding in 2004, it relaunched in 2011 and is still in operation today.

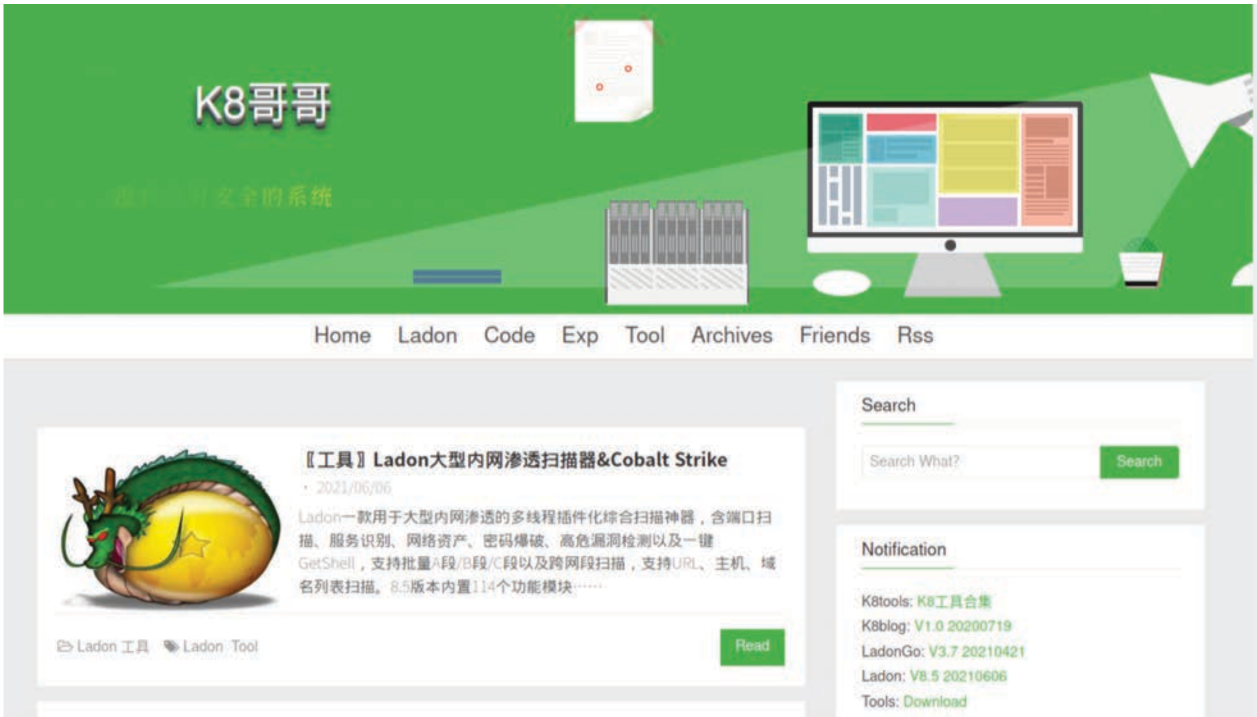
While the Chinese government condones patriotic hacktivism during times of international crisis, it also realizes that such activity is a double-edged sword, where the same tools and tactics could be used in domestic cybercrime that harms its national interest. Much like the Honker Union of China, many clearnet hacking forums closed down for various reasons, and some have relaunched with different content. In late 2019, as part of the Net Cleanup Campaign, the administrators of 独特论坛 (Dute Forum) were arrested and charged by authorities for running a website to distribute malware.[10]

Many other prominent hacking websites, including 华中帝国 (Central China Empire), 红蓝社区 (Red Blue Community), and 小七论坛 (Little Seven Forum) have all closed down during the past 2 years. More recently, 黑客啦 (Hei Ke La) forum was briefly closed and then reopened on June 7, 2021, with a note indicating that the newly relaunched forum is dedicated to network security technology and that illegal content is prohibited. It provides an email address as the point of contact to report any illegal activities. This practice is similar to some other relaunched hacking forums where the website’s administrators wanted to avoid a permanent shutdown by authorities and thus vowed to be vigilant of any illegal activities on the website. Despite challenges, many Chinese-language hacking forums, including China Floating Cloud Forum, CNSec, MoonSec, Hackbase, and 52 pojie, continue to operate.

Some of the malicious tools continue to be circulated in the underground even after the demise of the original forum. Here is a posting of a RAT from the defunct Central China Empire Forum with an enhanced backdoor.

In addition to hacking forums, the blogs of some possible gray-hat researchers also feature prominently in China’s information security world. One of them is from the threat actor “K8gege”, who hosts a blog and has established a GitHub software development platform repository under the same name. The repository contained numerous tools for hacking, such as privilege escalation, vulnerability exploitation, antivirus evasion, backdoors, network scanning, data exfiltration, and encryption or decryption. The threat actor updates the tools frequently to incorporate new features and newly released CVEs. One of the threat actor’s more well-known tools is the Ladon scanner and penetration tester, which works together with Cobalt Strike, as shown below:

[10] Dute Forum is permanently closed, website administrator under investigation! hxxps://www.anquanke[.]com/post/id/195010



【工具】Ladon大型内网渗透扫描器&Cobalt Strike

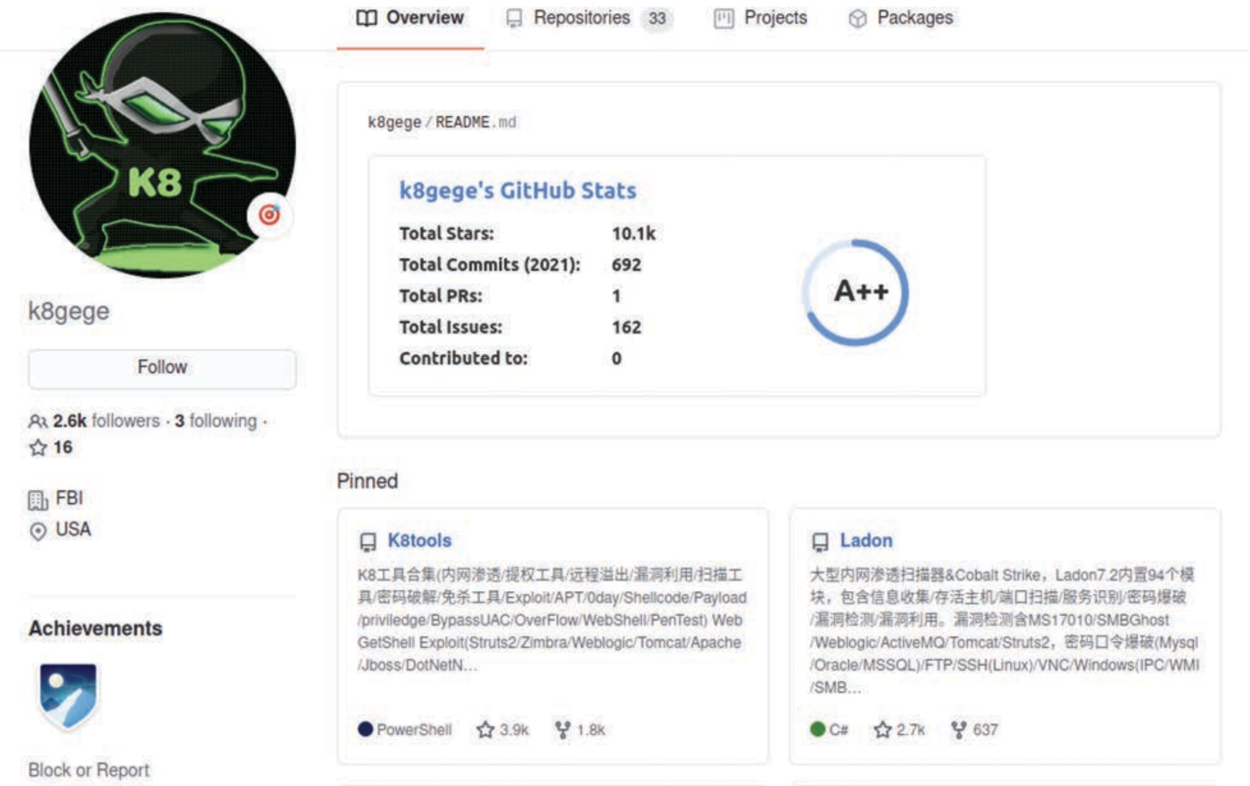
· 2021/06/06

Ladon一款用于大型内网渗透的多线程插件化综合扫描神器，含端口扫描、服务识别、网络资产、密码爆破、高危漏洞检测以及一键GetShell，支持批量A段/B段/C段以及跨网段扫描，支持URL、主机、域名列表扫描。8.5版本内置114个功能模块……

Notification

K8tools: K8工具合集
K8blog: V1.0 20200719
LadonGo: V3.7 20210421
Ladon: V8.5 20210606
Tools: Download

Figure 20: K8gege's blog website includes an introduction to the Ladon scanner and penetration tester. The description reads, "[Tool] Ladon Large-Scaled Internal Network Penetration Tester and Scanner with Cobalt Strike - Ladon is a large-scaled internal network penetrator tester and scanner with multi-thread plug-ins, it includes port scanning, service identification, network asset, password cracking, high-risk vulnerability detection and one-click GetShell, supports batched Class-A/B/C and inter-class scanning, supports URL, host, domain list scanning. Version 8.5 has 114 modules ..." (Source: Recorded Future)



k8gege

2.6k followers · 3 following ·
☆ 16

FBI
USA

k8gege / README.md

k8gege's GitHub Stats

Total Stars:	10.1k
Total Commits (2021):	692
Total PRs:	1
Total Issues:	162
Contributed to:	0

Pinned

K8tools

K8工具合集(内网渗透/提权工具/远程溢出/漏洞利用/扫描工具/密码破解/免杀工具/Exploit/APT/0day/Shellcode/Payload/priviledge/BypassUAC/OverFlow/WebShell/PenTest) Web GetShell Exploit(Struts2/Zimbra/Weblogic/Tomcat/Apache/Jboss/DotNetN...

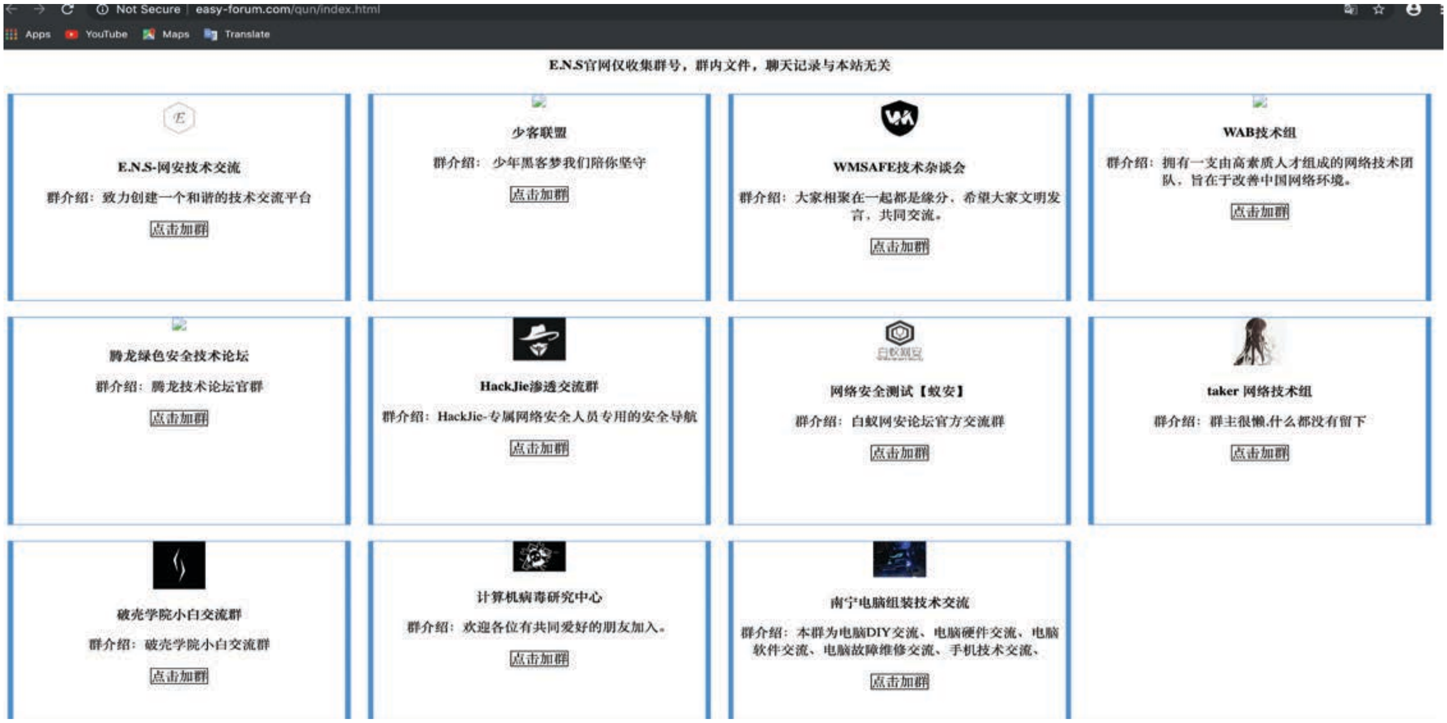
● PowerShell ☆ 3.9k 1.8k

Ladon

大型内网渗透扫描器&Cobalt Strike，Ladon7.2内置94个模块，包含信息收集/存活主机/端口扫描/服务识别/密码爆破/漏洞检测/漏洞利用。漏洞检测含MS17010/SMBGhost/Weblogic/ActiveMQ/Tomcat/Struts2，密码口令爆破(Mysql/Oracle/MSSQL)/FTP/SSH(Linux)/VNC/Windows(IPC/WMI/SMB...

● C# ☆ 2.7k 637

Figure 21: K8gege's GitHub repository, where the K8tools, a collection of the threat actor's penetration testing, privilege escalation, remote buffer overflow, vulnerability exploitation, scanning, password cracking and counter anti-virus tools, as well as the aforementioned Ladon scanner and penetration tester, are highlighted. (Source: Recorded Future)



E.N.S官网仅收集群号，群内文件，聊天记录与本站无关

E.N.S-网安技术交流
群介绍：致力创建一个和谐的技术交流平台
点击加群

少客联盟
群介绍： 少年黑客梦我们陪你坚守
点击加群

WMSAFE技术杂谈会
群介绍：大家相聚在一起都是缘分，希望大家文明发言，共同交流。
点击加群

WAB技术组
群介绍：拥有一支由高素质人才组成的网络技术团队，旨在于改善中国网络环境。
点击加群

腾龙绿色安全技术论坛
群介绍：腾龙技术论坛官群
点击加群

HackJie渗透交流群
群介绍：HackJie-专属网络安全人员专用的安全导航
点击加群

网络安全测试【蚁安】
群介绍：白蚁网安论坛官方交流群
点击加群

taker 网络技术组
群介绍：群主很懒,什么都没有留下
点击加群

破壳学院小白交流群
群介绍：破壳学院小白交流群
点击加群

计算机病毒研究中心
群介绍：欢迎各位有共同爱好的朋友加入。
点击加群

南宁电脑组装技术交流
群介绍：本群为电脑DIY交流、电脑硬件交流、电脑软件交流、电脑故障维修交流、手机技术交流、
点击加群

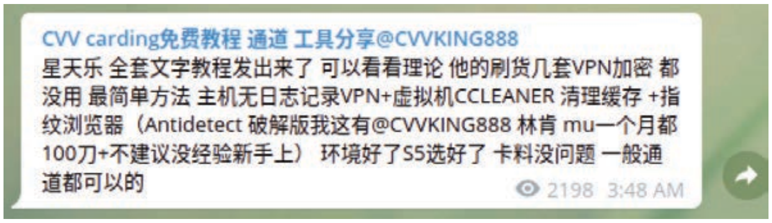
Translation: [Examples of security related QQ groups, from left to right, top to bottom]
ENS - Network Security Technology Exchange, Young Hacker Alliance,WMSAFE Technology Conversation Group, WAB Technology Group, Tamron Green Security Technology Forum, HackJie Penetration Communications Group, Network Security Testing (Termite Network Security), Taker Network Technology Group, Newbies Communication Group for Bash Shell Academy,Computer Virus Research Center, and Nanning Computer Assembly Technology Exchange

Figure 22: Examples of QQ groups that are related to information security, hacking skills, and malware research.

Instant Messaging Platforms

Instant messaging platforms native to China, such as Tencent WeChat and Tencent QQ groups, are also used by Chinese cybercriminals. Like their clearnet hacking forums counterparts, many of them operate under the guise of information security discussion groups while offering hacking tools and services. However, due to privacy concerns and fear of law enforcement, they are slowly losing popularity to overseas platforms such as Telegram and Jabber.

Telegram is becoming increasingly popular with Chinese cybercriminals due to its end-to-end encryption and anonymous nature. Many of the above-mentioned dark web marketplaces have accompanied Telegram channels that function as secondary communication channels. In addition, the threat actor "星天乐" (Xing Tian Le), a well-known carding threat actor in the Chinese-language underground, mainly operates on Telegram and offers CVV dumps and carding tutorials, which are widely traded.



CVV carding免费教程 通道 工具分享@CVVKING888
星天乐 全套文字教程发出来了 可以看看理论 他的刷货几套VPN加密 都没用 最简单方法 主机无日志记录VPN+虚拟机CCLEANER 清理缓存 +指纹浏览器（Antidetect 破解版我这有@CVVKING888 林肯 mu一个月都100刀+不建议没经验新手上） 环境好了S5选好了 卡料没问题 一般通道都可以的

2198 3:48 AM

Figure 23: A message in the Telegram Channel "CVV Carding Free Tutorial, Channel, and Tool Sharing @CVVKING888" where the carding tutorial of Xingtianle is shared. Some of Xingtianle's techniques include using a logless VPN on the host machine, using CCLEANER to clean the buffer on the virtual machine, and using a cracked version of Antidetect browser. (Source: Recorded Future proprietary data)

Migration to Established Criminal Sources

Threat actors skilled in hacking and who speak English or Russian have been observed on established and popular criminal forums including Exploit, Hack Forums, Raid Forums, and XSS. They advertise compromised payment cards, data dumps, malware, and other tools and services on those forums. In addition to being a GandCrab affiliate, the previously mentioned threat actor cnhack was last seen selling access to domain and workgroups on the private network of a Chinese manufacturing company on XSS.

Below are several examples of possible China-related offerings sighted on established criminal sources. While it is difficult to assess whether these are indeed China-based actors or overseas actors selling China-related data, one thing for certain is that the increase of these offerings signal that China-related content is becoming part of the global cybercrime landscape.

Source	Event
Raid Forums	On June 18, 2021, “MachineHooks” advertised unspecified network access methods to 3 China-based companies (the BTC prices are as of June 18, 2021): -China Electronics Technology Avionics Co., Ltd. (cetca.net.cn): access permits administrative control from external sources, including satellites and drones. The access also includes staff data. Priced at 0.5 BTC, or about $18,000. -China GWDR Power Technology: access from external sources and permits control of critical infrastructure, including the company’s internal power and control systems of bridges in 2 Provinces: Jiangsu and Zhejiang. Priced at 0.25 BTC, or about $9,000. -China Nanjing Quanxin Cable Technology Co., Ltd. (qx-kj.com): access control privileges from external sources to Chengdu J-20 simulator cockpit, radar target simulator, and integrated detector. Priced at 0.25 BTC, or about $9,000. (BTC to USD conversion rates are approximate and current as of the writing of this report.)
Exploit	On June 8, 2021, “inthematrix1” auctioned off admin access to an unspecified Hong Kong information technology company that provides IT and POS software solutions in the Asia-Pacific region. According to the threat actor, they compromised about 40 GB of corporate data, including PDF files and employee and customer information such as bank statements from 4 banks: HSBC, Citibank, Standard Chartered, and Bank of Ceylon. The threat actor stated that the corporate server hosts 2 organizations with headquarters in Hong Kong and China. The starting price for access was $4,000 or it could be purchased directly for $8,000.
Raid Forums	On February 22, 2021, “abs0009990s”, a member of the mid-tier Raid Forums, advertised 1.6 million bank records from the China-based bank Agricultural Bank of China (abchina.com) for $10,000 that included the following personally identifiable information (PII): full names, dates of birth, genders, physical addresses, and bank account numbers.

Outlook

Compared to their counterparts in other regions, Chinese cybercriminals operate under an even more challenging environment. Underground marketplace operators need to worry about everything from investing in robust servers to thwart potential government-sponsored DDoS attacks or interventions to ensuring the forum members do not expose themselves to draw attention from censorship or law enforcement. Meanwhile, cybercriminals need to take the necessary precautions to ensure anonymity, as well as constantly worrying about being ripped off by another party or the marketplace platform when conducting transactions. As a result, threat actors are willing to use throwaway handles across different forums to ensure anonymity at the expense of building an underground reputation. Many cybercrime marketplaces and forums also declare support for the Chinese Communist Party and vow to ban illegal activities to avoid unwanted attention from the government. The general lack of structure and trust in the cybercrime underground further promotes the "every man for himself" mentality.

As the heavy-handed, high-tech surveillance of Uyghur Muslims in Xinjiang, from mobile hacking tools used for location tracking to big data-driven facial recognition programs, is being exposed to the world, there is little doubt that the same TTPs could be soon carried out in other parts of China. Despite the omnipresence of the Great Firewall, the banning of Tor service and Telegram, as well as the frequent law enforcement crackdowns, the Chinese cybercrime underground still finds a way to thrive. The constant game of 道高一尺、魔高一丈 ("one-upmanship") between the government and cybercriminals will be undoubtedly be going on for the foreseeable future.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.