Recorded Future

CYBER THREAT ANALYSIS

Thieves and Geeks: Russian and Chinese Hacking Communities

By Winnona DeSombre and Dan Byrnes
Recorded Future

CTA-2018-1010

Scope Note: Recorded Future's Insikt Group analyzed advertisements, posts, and interactions within hacking and criminal forums to explore the capabilities, cultures, and organization of Chinese and Russian hacking communities. Sources include the Recorded Future product, as well as Russian and Chinese personas created by Recorded Future to interact with actors on these forums.

This report will be of greatest interest to organizations seeking to understand the criminal underground to better monitor industry- and company-specific threats, as well as to those investigating the Russian or Chinese criminal undergrounds.

Executive Summary

When researchers primarily focus on items being sold on dark web markets, many gloss over the various types of communities that reside within the forums themselves, either focusing solely on Russian hacking collectives or not talking about forum members at all. This can cause readers to assume that the "hacker community" is an amorphous collective of individuals transcending borders and cultures. Quite the opposite — each country's hackers are unique, with their own codes of conduct, forums, motives, and payment methods. Recorded Future has actively analyzed underground markets and forums tailored to Russian and Chinese audiences over the past year and has discovered a number of differences in content hosted on forums, as well as differences in forum organization and conduct.

Key Judgments

- Both Russian and Chinese forums host a wide variety of international content. While it is uncommon for Russian forums to advertise data dumps from Russian companies, data dumps and malware originating from Chinese companies are usually only found on Chinese forums.
- Chinese speakers are active on Chinese, English, and Russian forums, while few to no Russian or English speakers use Chinese forums.
- Although current Chinese posts on non-Chinese forums are tailored to Chinese buyers, Recorded Future assesses with low confidence that Chinese buyers are beginning to bring services, data, and malware once unique to Chinese forums to a more international audience.

- Russian forums will likely continue to provide content to a wide set of buyers on the internet in order to generate as much revenue as possible.
- Russian forums are more tailored to business transactions, while Chinese forums instead focus on building the Chinese hacking community. Both communities sell goods and services for regional users, although this is far more prevalent on Chinese forums.
- Hacktivism originating from China as a result of politically sensitive international events has continued even after the dissolution of the original patriotic hacking groups and is likely to continue in the future.

Analysis

Russian Forums — Thief Spirit

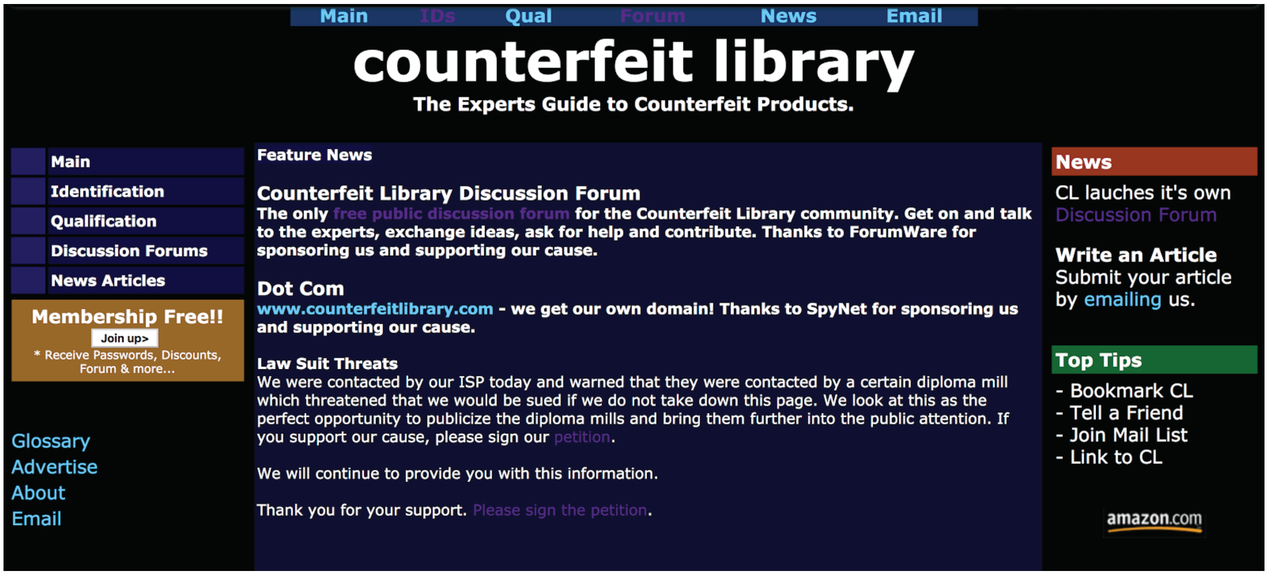
Chinese and Russian hacker groups, while emerging from similarly authoritarian countries, have very different origin stories and operate in different ways. Russian-speaking cybercriminals hold one thing above all else: money. Although sophisticated cybercrime is a trademark of the former Soviet Bloc, the financially-motivated cyber underground has much of its roots in the United States.

In 2000, the underground forum Counterfeit Library emerged as one of the first carding and fraud forums for English speakers.[1] Russian speakers, upon discovering Counterfeit Library, wanted their own version, and responded with the "Odessa Summit." This summit brought together a group of around 20 of the most premier Ukrainian fraudsters, who later became the founders of the Russian-language "Carders Alliance," or simply CarderPlanet.[2] CarderPlanet implemented a hierarchy of moderators and vetted all vendors before allowing them to sell any dumps, CVVs, fulls,[3] SSNs, eBay accounts, magnetic stripe encoders, or skimmers — all the staple products of the carder community.

Following the lead set by CarderPlanet, the English-speaking world responded with ShadowCrew, another carding forum catered to

[1] Poulsen, K. Kingpin. Broadway Books. 2011.
[2] Ibid
[3] Personally identifiable information used for financial fraud.

Western fraudsters with the professionalism and structure of the Russian-speaking underground.[4] Later, in 2005, the opening of CardersMarket allowed Western and Eastern fraudsters to conduct business with each other in the same forum.[5]



counterfeit library

The Experts Guide to Counterfeit Products.

Feature News

Counterfeit Library Discussion Forum

The only free public discussion forum for the Counterfeit Library community. Get on and talk to the experts, exchange ideas, ask for help and contribute. Thanks to ForumWare for sponsoring us and supporting our cause.

Dot Com

www.counterfeitlibrary.com - we get our own domain! Thanks to SpyNet for sponsoring us and supporting our cause.

Law Suit Threats

We were contacted by our ISP today and warned that they were contacted by a certain diploma mill which threatened that we would be sued if we do not take down this page. We look at this as the perfect opportunity to publicize the diploma mills and bring them further into the public attention. If you support our cause, please sign our petition.

We will continue to provide you with this information.

Thank you for your support. Please sign the petition.

News

CL lauches it's own Discussion Forum

Write an Article

Submit your article by emailing us.

Top Tips

- Bookmark CL
- Tell a Friend
- Join Mail List
- Link to CL

The homepage of the original fraud and carding forum, Counterfeit Library.

During these early years in the formation of the cybercriminal underground, much of the activity surrounding credit card fraud, phishing, spamming, and the like was conducted by Americans. This is evidenced by the number of big busts and takedowns, such as Operation Firewall, Operation Shrouded Horizon, and the DarkMarket takedown, which dismantled many of the serious Western carder communities.

In Eastern Europe, technology use spread more slowly, and it took more time for internet connectivity and the personal computer to become ubiquitous in the republics and federations of the former USSR. The well-educated and underpaid citizens of these countries turned to crime against the West because they had the technical skills and needed the money. This is evidenced in the explosion of the types of scams, fraud, and malware launched by Russians in the early 2000s. For example, "Webmaster" forums such as Crutop and Master-X emerged with a focus on driving traffic to countless niche porn sites. Rogue pharmaceutical affiliate

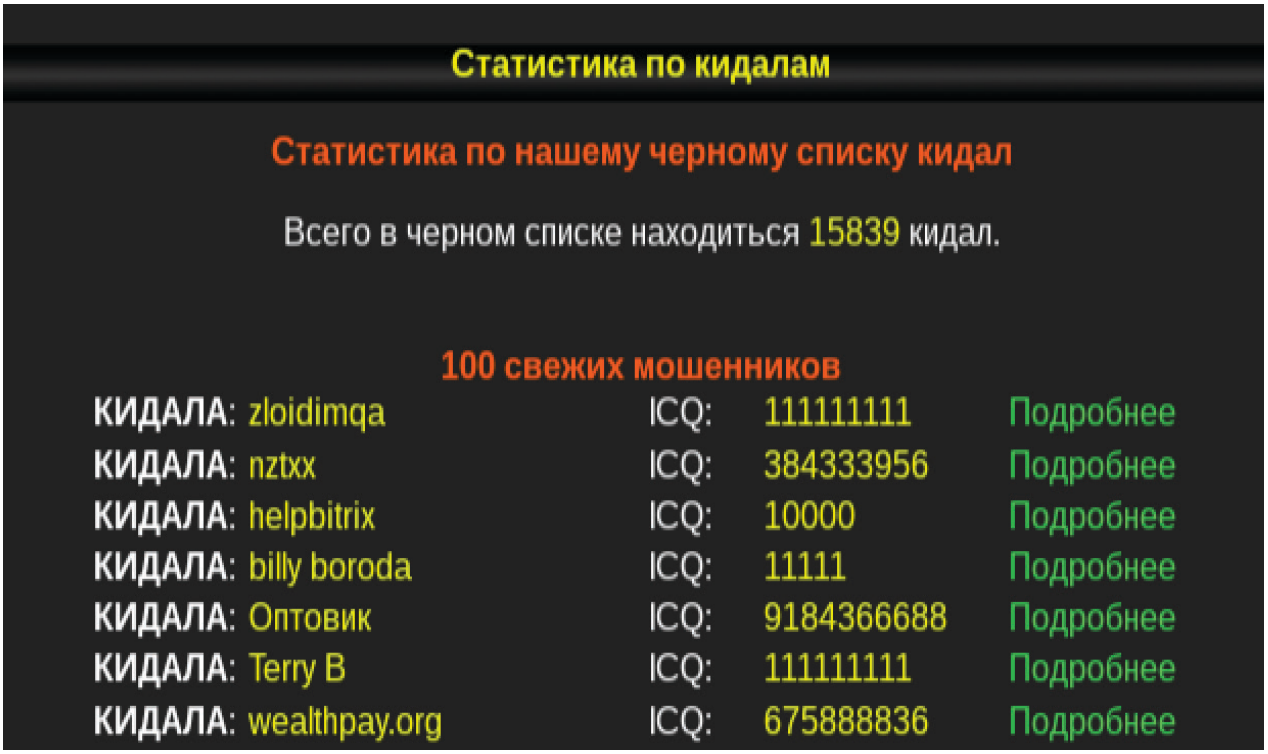
[4] Poulsen, K. Kingpin. Broadway Books. 2011.
[5] Ibid.

programs (or "partnerkas") such as GlavMed and Rx-Promotion paid affiliates to spam out ads for erectile dysfunction medications and antidepressants. Pyotr Levashov, also known as Severa, operated rogue antivirus partnerkas, referral programs that deceived victims into buying useless software claiming to clean up infected computers, in addition to spreading the infamous Waledac and Kelihos botnets. The JabberZeuS Crew, the Business Club, and other crime rings collectively pocketed over $200 million from U.S. and U.K. financial institutions using Evgeniy Bogachev's ZeuS banking trojan before law enforcement could put a stop to it. These are only a small fraction of the cyber underground's economic success stories, and there is little indication of it slowing down.

Current Landscape

Russian forums leave very little room for socializing or camaraderie. These sites are places of business, not bastions for community. Respect and trust are built on successful financial transactions, and the reliable, consistent forum members rise to the top of their trade, while those with lesser consistency are given poor ratings. Members with poor ratings or bad reviews often end up on the forum's blacklist and can be sentenced to a role as a "kidala" or "ripper," meaning an individual who rips off others. There are no apprentices in this corner of the dark web, and few Russian forum members are willing to teach anyone anything without clear financial benefit.

Despite being focused on business, successful members offer useful tools and good customer service. Carders who deal in bulk and provide good customer service, such as refunding declined credit cards in a timely manner, are preferred and rewarded with loyal buyers for as long as the supply lasts. Sellers of trojans and spam services give out holiday discounts, and bulletproof hosters pay referral bonuses to any existing customers who send them new business. These actors operate with the financial wit of the major corporations they themselves so often target.



Статистика по кидалам

Статистика по нашему черному списку кидал

Всего в черном списке находиться 15839 кидал.

100 свежих мошенников

КИДАЛА:	zloidimqa	ICQ:	111111111	Подробнее
КИДАЛА:	nztxx	ICQ:	384333956	Подробнее
КИДАЛА:	helpbitrix	ICQ:	10000	Подробнее
КИДАЛА:	billy boroda	ICQ:	11111	Подробнее
КИДАЛА:	Оптовик	ICQ:	9184366688	Подробнее
КИДАЛА:	Terry B	ICQ:	111111111	Подробнее
КИДАЛА:	wealthpay.org	ICQ:	675888836	Подробнее

Kidala is a website dedicated entirely to tracking the rippers of the criminal underground — 15,839 and counting.

There have been multiple instances of Russian hackers engaged in patriotic, vigilante activity, such as the cyberattacks against Estonia, Georgia, and others deemed personae non gratae by the Russian Federation. According to a study by Arbor Networks titled "Politically Motivated Distributed Denial of Service Attacks," the pro-Kremlin youth group Nashi was allegedly involved in a DDoS attack against Estonia after a Soviet monument was removed.[6] There was also a DDoS bash script made publicly available on the Russian blogging site LiveJournal whose function was to ping flood a list of Estonian IPs, allowing the less technical actors to get into the fight. The study also found that during the brief Russo-Georgian war, a DDoS attack was launched in sync with Russian tanks from various BlackEnergy-based botnets. One source claims that the spammer, Peter Levashov (Severa), sent out spam messages slandering the Kremlin and Mikhail Prokhorov, and recruited hackers to the "Civil Anti-Terror" community, which targeted Islamist and Chechen-separatist websites.[7] Other, more verifiable accounts of Kremlin-backed hackers include Karim Baratov and Alexsey Belan, who were recruited by the FSB to orchestrate the Yahoo breach beginning in 2014.

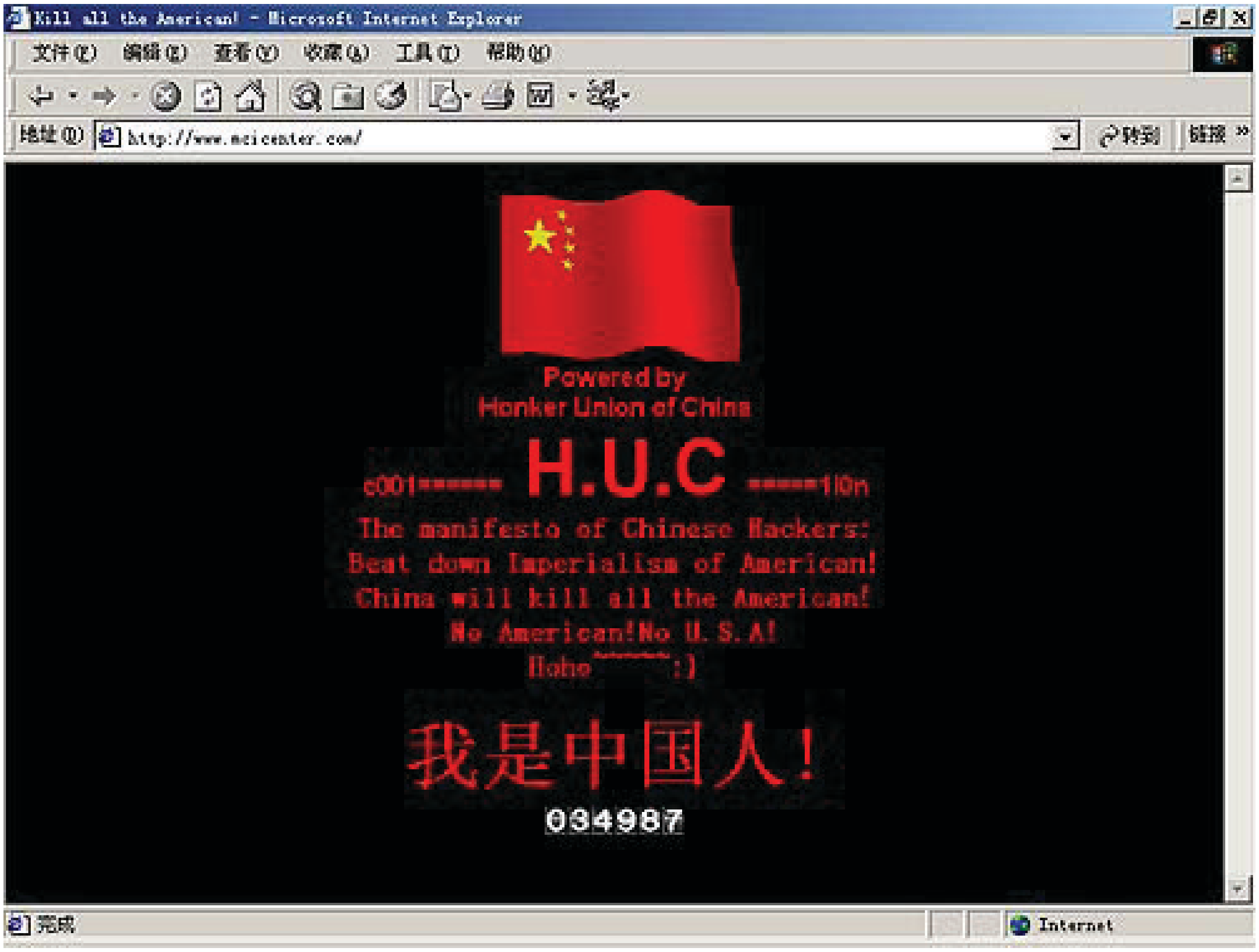
[6] Nazario, Joes. *Politically Motivated Denial of Service Attacks*. 2008.
[7] Shnygina, Anna. "'It's our time to serve the Motherland' How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers." 2018.

Chinese Forums — Geek Spirit

Unlike Russia's underground hacking community, many of China's first hackers rallied around patriotism.[8] Much of this sentiment originated from China's national determination to never relive its "century of humiliation" from the late 1800s and early 1900s, during which it was coerced by other great powers into unequal treaties, concessions, and a forced opium trade.

China's first hacker groups emerged in the late 1990s, triggered by anti-Chinese riots in Indonesia. Chinese netizens expressed outrage at the international community for treating their fellow citizens with contempt and set up discussion boards, social media groups, and bulletin board systems to plan defacements against Indonesian government websites. Many of these boards evolved into the first Chinese hacking groups: the Green Army, China Eagle Union, and Hongke (or Honker) Union. These groups all contributed to early internet defacements, DDoS attacks, and credential thefts targeting the U.S. and other Chinese adversaries. One such attack was in May of 2001, when the Hongke Union famously DDoSed the White House site and targeted websites of U.S. businesses in retaliation for the collision between a U.S. spy plane and a Chinese fighter jet off of Hainan Island that occurred a month earlier.

[8] Henderson, Scott J. *The Dark Visitor*. 2007.


Kill all the American! - Microsoft Internet Explorer
文件(F)
编辑(E)
查看(V)
收藏(A)
工具(T)
帮助(H)
地址(D)
http://www.mcicenter.com/
转到
链接 »
完成
Internet

Powered by
Honker Union of China
c001====== H.U.C =====10n
The manifesto of Chinese Hackers:
Beat down Imperialism of American!
China will kill all the American!
No American!No U.S.A!
Hoho^^^^^^^ :)
我是中国人！
034987

Defacement of a U.S. website by Hongke (or Honker) Union group.

While all three of these original groups have either shut themselves down, splintered, or faded away, this initial wave of cyber patriotism enabled a robust government-hacker relationship in China. Individuals have been recruited into government positions from Chinese technical forums, and many famous old-school hackers now run large cybersecurity and technology firms in China's flourishing cybersecurity market while maintaining excellent business relationships with the Chinese government. Numerous Chinese cybercriminals have also admitted to contracting their services to national intelligence agencies and military organizations like the Ministry of State Security or the People's Liberation Army.

Although many have also been turned into security news forums, patriotic hacking sites do still exist. Historically, Chinese hacktivist activity tends to increase noticeably whenever geopolitically sensitive events occur in the East Asian region. Chinese hacktivist groups have reemerged to deface sites in countries involved in disputes with China over islands in the South and East China Seas. In 2012, 300 Japanese organizations were listed as targets for defacement on the message board of a Hongke Union-affiliated web page (eight years after the Hongke Union's leaders had officially called for the group's disbandment) to proclaim Chinese sovereignty over the Diaoyu Islands, a subject of intense diplomatic dispute between China and Japan during that time.

A new hacktivist group, 1937CN, initially compromised websites in Vietnam in May 2014 after Vietnamese outrage over a Chinese oil rig deployed in Vietnamese territorial waters. After primarily defacing websites in the Philippines in late 2015, 1937CN famously compromised the check-in systems at multiple major Vietnamese airports in July 2016, exposing the personal data of approximately 411,000 passengers in the process. This was allegedly a patriotic response to Vietnam's relocation of missile launchers to disputed islands in the South China Sea.

It is difficult to determine how independently these hackers are acting. Malware found during the 1937CN's Vietnamese airport compromise has been linked to wider, possibly state-sponsored cyberespionage campaigns against Vietnamese organizations. However, the group also seems to contain elements of hacktivism. 1937CN has a Zone-H web defacement account, various social media accounts linked to their website, and even a promotional video consisting of multiple hooded individuals wearing Guy Fawkes masks, uploaded to a popular video-sharing site in July 2017.[9] Additionally, the Chinese government took down 1937CN's website in March 2017, which it has done in the past to websites of other Chinese hacker groups that too aggressively pursue perceived slights to China's reputation.

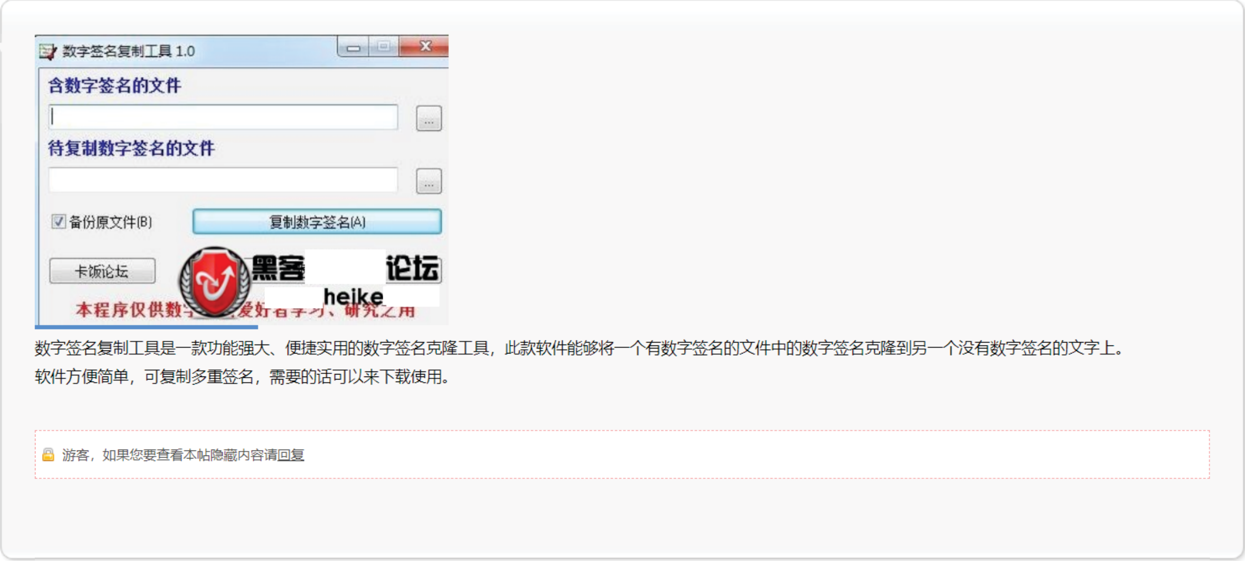
Current Landscape

Chinese forum members feel an overwhelming sense of community online. The term "geek spirit" (极 客精神) is used to denote forum culture and refers to groups of technical individuals who hope to

[9] While also known as the symbol of international hacking collective Anonymous, the Guy Fawkes mask was popularized by 2005 film *V for Vendetta*, widely thought to be banned in China until 2012.

create a more ideal society. Many of these forums require members to engage with a post, either through a comment or personal message, before being able to purchase or trade malware. Daily interaction on a forum can also be a prerequisite for maintaining forum membership or a way to generate in-forum currency — money specifically held inside the forum used to buy products and added to by outside sources such as Bitcoin and Alipay.

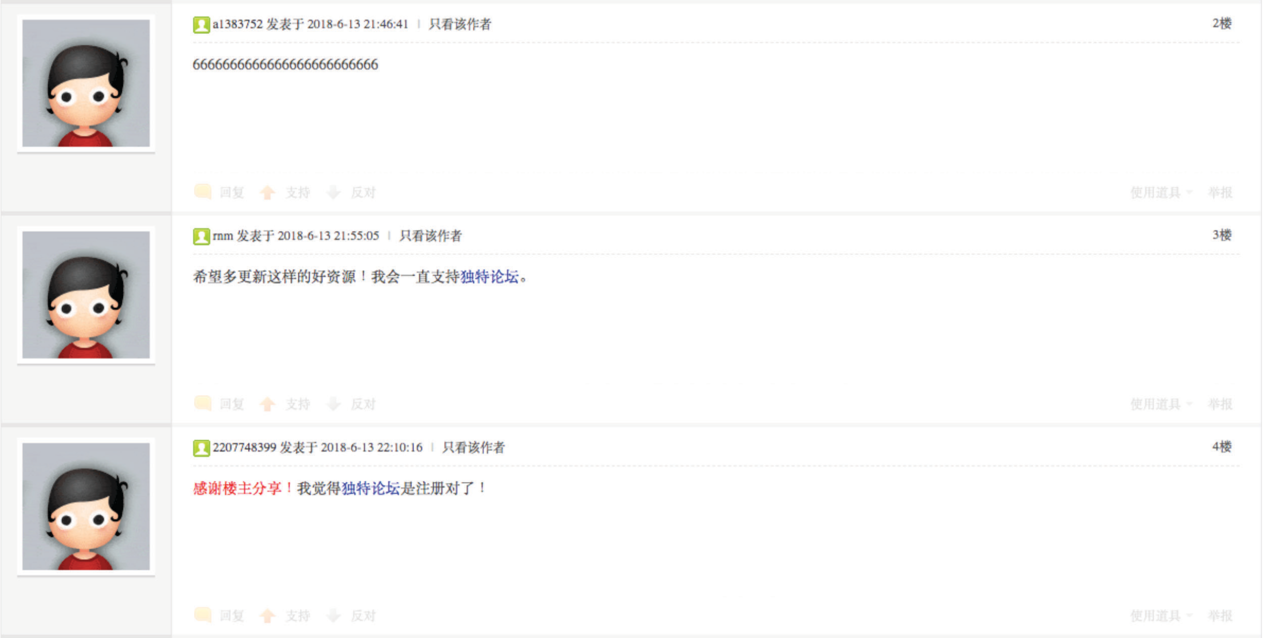
This required social interaction with other forum members builds community; comments within forums range from slang praising the tools written by advertisers, to messages thanking the seller outright. In addition, Chinese hackers advertise applications for apprenticeship programs on similar forums, where a more experienced hacker will teach an apprentice for a fee, dividing work among members based on skill level. Potential hackers will also ask for tutelage to get more involved in the community. This willingness to teach and social engagement is in stark contrast to the norms on Russian language forums that we detailed above.



数字签名复制工具是一款功能强大、便捷实用的数字签名克隆工具，此款软件能够将一个有数字签名的文件中的数字签名克隆到另一个没有数字签名的文字上。软件方便简单，可复制多重签名，需要的话可以来下载使用。

🔒 游客，如果您要查看本帖隐藏内容请回复

Forum post requiring a "回复," or reply, before a user can gain access to software that copies digital signatures.



a1383752 发表于 2018-6-13 21:46:41 | 只看该作者 2楼

6666666666666666666666666

rnm 发表于 2018-6-13 21:55:05 | 只看该作者 3楼

希望多更新这样的好资源！我会一直支持独特论坛。

2207748399 发表于 2018-6-13 22:10:16 | 只看该作者 4楼

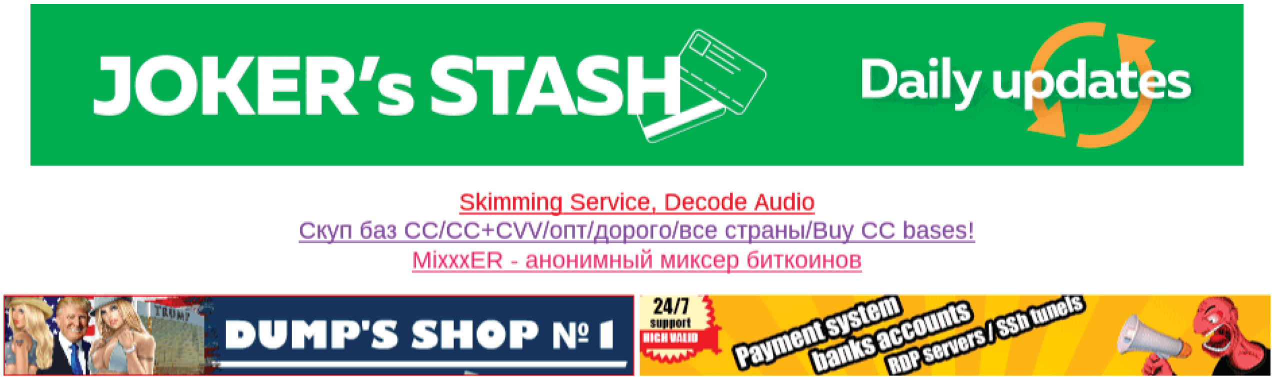
感谢楼主分享！我觉得独特论坛是注册对了！

Encouraging replies on a forum thanking a user for sharing a custom tool.

Organization of Russian Underground Forums

The social dynamics within the Russian criminal forums are fairly compartmentalized and professional. This is exemplified by the fact that Russian fraudsters and Russian hackers largely operate on different forums. Fraud and carding forums are focused on the sale of stolen financial information, while hacking forums have more of a focus on malware, exploits, and other technical tools. Among general hacking forums, three main tiers of forums have evolved: open, semi-private, and closed. Open forums are largely available to all users, requiring only a functional email account for registration. Semi-private communities have some threshold for entry, such as a $50 registration fee or proof of membership on other boards. The administrators of more prestigious “closed” forums require those applying for membership to prove the authenticity of the illicit services they offer and/or require current forum members to vouch for them. Other forums like Exploit require users to have a certain number of posts to see more sensitive content.

Historically, these forums have been accessible on the clearnet, but many have adopted Tor mirrors as both a backup and a separate means of access for those without virtual private networks (VPNs). The forum administrators for Verified moved to Tor entirely in 2018 due to difficulties staying online on the clearnet, cycling through multiple top-level domains and hosts. Other criminal resources, like the carding shop Joker's Stash, have adopted blockchain DNS, utilizing a decentralized approach to their carding operation and resilience against traditional takedown efforts.



Skimming Service, Decode Audio
Скуп баз CC/CC+CVV/опт/дорого/все страны/Buy CC bases!
MixxxER - анонимный миксер биткоинов

Banner ads posted in English and Russian from the forum Korovka.

Russian fraudsters and hackers do not rely on the traditional banking system to facilitate payments. Some of the original digital currency systems, like the now defunct E-gold, ePassporte, and Liberty Reserve, required little more than a valid email address to transfer stolen money into usable bank accounts and debit cards. For well over a decade, WebMoney was the go-to method of payment used on the Russian forums, but Recorded Future has since observed a substantial decline in its use since the rise in cryptocurrency. Presently, Bitcoin, Monero, and other cryptocurrencies have been widely adopted in the Russian underground forums, and a cottage industry of cashout services have cropped up to exchange those coins into dollars or rubles. Money laundering operations like Fethard and ChronoPay are also used on top of cryptocurrencies, as the operations utilize an ever-changing network of banks and front companies to cover the final destination of currency used in illicit transactions.

Russian cyber outlaws must abide by an unwritten law if they desire to remain in front of their computer screens instead of a judge at the Moscow City Court: do not target citizens of the Commonwealth of Independent States. While Eastern Bloc cybercriminals have been known to test their malware on the domestic population before turning their cyber weapons toward Western targets, offenders who do more than just testing are quickly arrested. Dmitry "Paunch" Fedotov used his Blackhole exploit kit to spread multiple forms of malware internationally, but was only arrested when he started spreading malware for the Carberp gangs, who made their living targeting Russian citizens. Pavel Vrublevsky, owner of Russian payment processing service ChronoPay, provided money laundering and logistical services for illegal pharmaceutical sales and rogue antivirus without Russian government intervention, but he was arrested after ordering a DDoS attack on the rival Russian payment processor Assist. Recorded Future has and still sees many Russian hackers who specifically state that their malware is not to be used against Russians or members of the CIS.

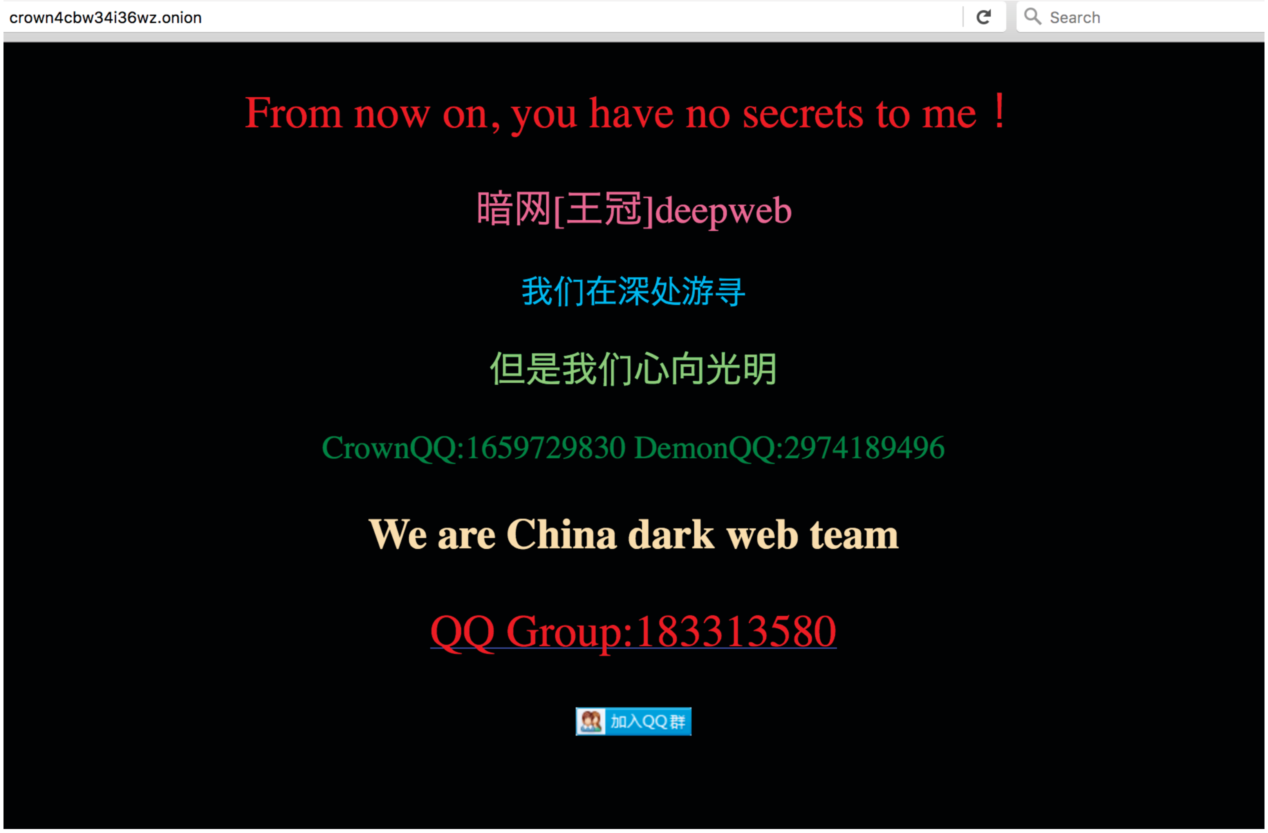
Organization of Chinese Underground Forums

Chinese hacker groups are organized in notably different ways to their Russian counterparts, partially due to China's strict censorship regime. The Golden Shield Project, or what would later become known as the "Great Firewall of China," has been run by China's Ministry of Public Security since 2000. The project was initially conceptualized to promote the adoption of advanced technology to strengthen central police control, responsiveness, and crime combating capacity. However, much of the project evolved over time to focus on content-filtering for Chinese individuals through IP blocking, IP address misdirection, and data filtering as internet adoption spread quickly throughout China.

The Great Firewall blocks websites, apps, social media, emails, messages, VPNs, and other internet content determined by the Chinese state to be inappropriate or offensive. For Chinese hackers, this often makes searching for foreign hacking content or illegal content for sale difficult. Additionally, the Great Firewall has multiple methods to identify outgoing Tor connections and shut down use of the Tor network, where many underground forums and marketplaces reside. One of the only consistent ways to "跳墙,“ or jump the Great Firewall, is for Chinese citizens to use a VPN.

However, as of 2017, China's Ministry of Industry and Information Technology (MIIT) requires VPN providers in China to be licensed by Chinese officials, and has subsequently shut down many VPNs it claimed to be "unauthorized." This further stunts the ability of Chinese hackers to anonymously search the web or find international hacking sources. Because jumping the Great Firewall is so difficult, far fewer Chinese forums or marketplaces are hosted on Tor than their Russian or English counterparts; instead, Chinese hackers have developed their own communities based loosely on their original domestic patriotic hacking groups, and have set up a wide variety of lower-level hacking forums easily available on the Chinese internet.

In addition to these online communities, many hackers heavily utilize invite-only chat groups or forums within Chinese social media apps QQ, Baidu, and WeChat. However, native Chinese chat groups and forums are also heavily censored and occasionally shut down by the Chinese government. The government has shut down multiple hacking and fraud sites in the past for various legal reasons. Some QQ groups still advertised on dark web sites are no longer accessible, and searches for Tieba bars that housed known hacker activity also show up as banned. Furthermore, because the Chinese government has historically driven hacking activity through both formal and informal channels, many Chinese forum members are fully aware of the consequences of acting outside that informal agreement and usually stay away from targeting systems within their homeland.



From now on, you have no secrets to me！

暗网[王冠]deepweb

我们在深处游寻

但是我们心向光明

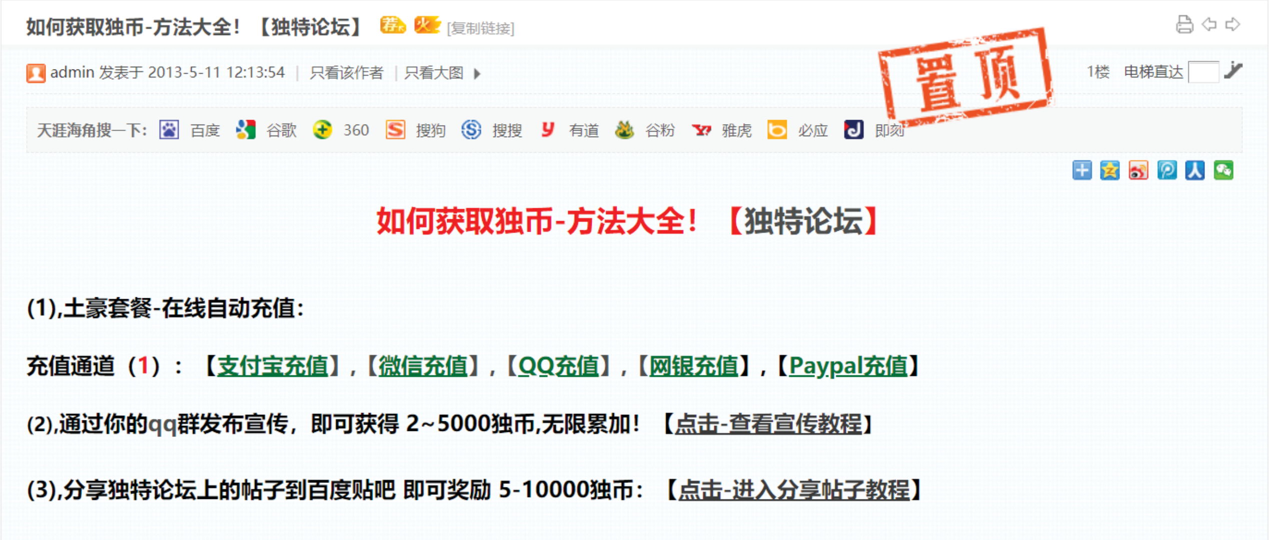
CrownQQ:1659729830 DemonQQ:2974189496

We are China dark web team

QQ Group:183313580

Onion site showcasing a QQ group that no longer exists.

Many Chinese entry-level forums also do not use Bitcoin due to China’s de facto ban of cryptocurrencies. China banned domestic initial coin offerings (ICOs) in September 2017, is actively blocking foreign cryptocurrency exchanges from domestic access, and has prevented Chinese financial institutions from conducting any Bitcoin transactions since 2013. To address the difficulty of obtaining Bitcoin in China, Chinese forums accept payments such as Alipay or Chinese bank transfers. Members can also generate forum currency by interacting with posts.



如何获取独币-方法大全！【独特论坛】

admin 发表于 2013-5-11 12:13:54

如何获取独币-方法大全！【独特论坛】

(1),土豪套餐-在线自动充值:

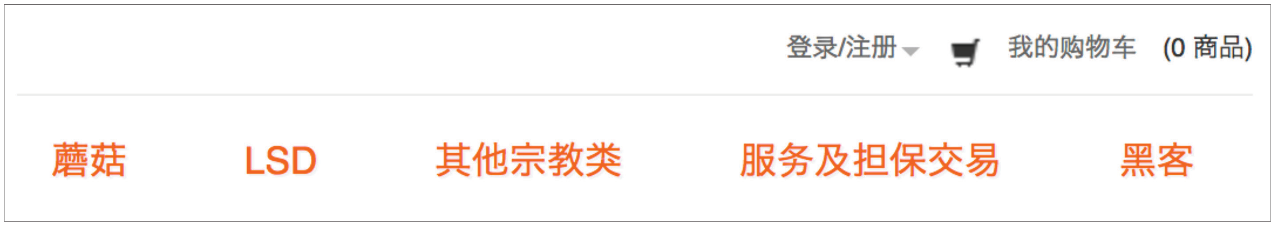
充值通道（1）：【支付宝充值】,【微信充值】,【QQ充值】,【网银充值】,【Paypal充值】

(2),通过你的qq群发布宣传，即可获得 2~5000独币,无限累加！【点击-查看宣传教程】

(3),分享独特论坛上的帖子到百度贴吧 即可奖励 5-10000独币：【点击-进入分享帖子教程】

Admin post on Chinese forum stating that the forum accepts payments through Alipay, WeChat, QQ, online banking, and PayPal. A forum member has the option to share this post on multiple Chinese social media outlets.

Chinese forums are also usually not as compartmentalized as their Russian counterparts, and are more community focused rather than business focused. Fraudsters and exploit writers will often use the same forums (albeit advertising their wares in different channels within the forum) and Chinese marketplaces dedicated to specific items like drugs or pornography will also contain a “hacker” section. Additionally, many underground forums for erotic content will also advertise “cracked web cameras” — cameras in bathrooms or bedrooms that have been broken into by amateur hackers. Member accounts on many forums have also been somewhat gamified: Chinese accounts are sometimes associated with levels — numbers correlated with how often an account logs onto a forum, the number of sales posts from an account, and whether the account has ever violated any forum rules. Chinese forums can encourage users to interact and share more online. This is similar to Russian forums, which require a user to surpass a set number of forum posts in order to view certain content. However, while both Russian and Chinese forums will also offer VIP-only channels and content as rewards for consistent forum interaction, Chinese forums will also offer in-forum currency, as mentioned above.



Menu of drug website with a section for "hackers" next to sections for mushrooms and LSD.

In general, Chinese forums and marketplaces are organized similarly to the three tiers (open, semi-private, and closed) of Russian forums. As with Russian forums, the quality and complexity of the products sold on the more open forums are usually not as good as products on their closed counterparts. This is usually due to the difference in vendor sophistication and reliability. Forums in both languages also contain an administrator-verified "blacklist" section, where individuals can post proof that a vendor has provided a faulty or deliberately false product or service. This usually provides a good enough deterrent against unreliable vendors. The forums with higher barriers to entry usually result in more experienced vendor membership simply by having a vetting process. While most vetting processes are explicit — paying a forum admin, proving access to other forums, or having an existing forum member sponsor the new member — some Chinese forums also have implicit vetting processes. For example, many Chinese hacker QQ group and WeChat group numbers are advertised on semi-private forums, meaning that one must have been pre-vetted by a different forum prior to gaining access to the group itself.

Another implicit vetting process a Chinese forum can employ is to simply host the forum on Tor. Many Chinese forums hosted on Tor only require an email for registration, but all Chinese users must be able to jump the Chinese firewall and understand how to find the forum in order to register. This likely contributes to why most users of these forums are more technical than users on the Chinese clearnet.

Content in Russian Underground Forums and Marketplaces

Malware

Malware on Russian forums has rapidly evolved, but forum tradecraft has largely stayed the same. Ransomware, loaders, trojans, exploit kits, installs, spam bots, web traffic, forged documents, money mules, bank accounts, and credit cards are all still present and accounted for — they just look a bit different. For example, rogue antivirus has evolved into scareware, then from scareware to lockers, from lockers back to scareware, and finally, from scareware to ransomware. Each type has its own flavor, but all render a victim's computer useless until hackers are paid to go away. The exploit kits Blackhole, Phoenix, and Nuclear have all come and gone, championed today by Rig, Magnitude, and Grandsoft. One of the few significant differences in tradecraft today is that malware is more likely to be dropped from weaponized Word macros than the once-dominant exploit kits.

ZeuS persists to this day across Russian malware forums as a trojan blueprint, despite its takedown in 2014. The leak of its source code was used to build a plethora of banking trojans like SpyEye, Dridex, and Carberp, and its lineage still survives to this day as Tinba and others. While banking trojans are certainly still in play, groups like FIN7 cut out the middleman and target banks directly. Although their top three members are in jail, Recorded Future believes the remaining members of Combi Security have potentially learned enough from their former managers to pose a threat to financial institutions in days to come.

Because the release of source code can increase the number of vendors selling the same or derivative malware like ZeuS's descendants, malware source code is carefully guarded by its authors. Malicious programs on the underground, like banking trojans and loaders, are sold in the form of "builds," which are similar to individual software licenses. For example, Smokebot, sold by the actor SmokeLdr, costs $400 per license, with the option to purchase additional modules, such as a form-grabber for $300 and a cryptominer for $100. There are even terms of agreement stating that each build (license) is only for one individual and is not to be resold. Rebuilds of Smokebot, or modification of the configuration file, are an additional $10 each, and are necessary if the customer needs to add a new command-and-control server in the case of a takedown or blacklisting. Only SmokeLdr has the ability to update the program's configuration, as the actor is the only one with the source code. All of these facets — full control of the source code, the additional modules, and the eventual need for rebuilds — allow for maximum monetization of Smokebot and are common practice throughout the Russian underground.

Partnerkas, or affiliate programs, are also employed by malware authors to maximize their revenue from a single piece of software. This method is used by ransomware strains like Cerber, operated by the threat actor crbr, who distributes builds of Cerber to the affiliates, or actors participating in the partnerka. These affiliates then spread Cerber themselves through vectors like spam or malvertising, and in return, earn a percentage of every ransom paid. A partnerka setup like this one allows crbr to focus primarily on the development of Cerber and its infrastructure, while outsourcing all the distribution to third parties without sharing the source code with anyone else.

Fraud

Dealing in fraud often means dealing in bulk quantities of information. The Target and Home Depot attackers absconded with the data of 40 and 56 million payment cards, respectively. Selling this many cards on forums or over Jabber chats would be a herculean labor, requiring a large support staff operating around the clock. To solve this problem, automated vending sites (also referred to as "carding shops") like Rescator, Trump's Dumps, and Joker's Stash were created to allow carders to order the specific types and quantities of credit and debit card data without any human interaction at all. These have a layout similar to Amazon or Ebay, where buyers can point and click on what they want, add it to their cart, and check out within a matter of minutes. Without carding sites such as these, it would be extremely difficult to monetize the massive amounts of data stolen from mega breaches.

Other fraud-related services require a much more personal touch. Criminals of all sorts often require fake identification in the form of driver's licenses, IDs, and passports, all of which can be found on Russian forums. The actor vengativo offers one such service, claiming that the fraudulent documents they sell are indistinguishable from the real things. This actor sells ID cards from dozens of European countries costing as much as $400, passports for countries such as the U.S. and Germany for $2,000, and even fake diplomas from Lithuanian universities. Believable identification documents are essential for fraudsters looking to make in-store purchases of high-value electronic devices with stolen payment cards, or open a bank account in a foreign country for money laundering.

Miscellaneous: Bulletproof Hosting and VPNs

Criminal forums, Jabber servers, banking trojans, and other criminal operations all could not exist without hosting, and those individuals who use these services could not use them securely without some sort of network anonymity. Thus, bulletproof hosting — hosting services operating in jurisdictions that large tech companies and federal law enforcement have no influence over — form the backbone of the criminal underground. Actors like Whost, who has been in business for over a decade, offers servers in Beirut, Lebanon for as little as $100 per month. The fast-flux hosting services operated by actors like Yalishanda make takedown efforts against malware extremely difficult, allowing infrastructure like CnC domains to be constantly cycled through ever-changing series of IP addresses. Additionally, VPNs allowing actors to hide their true IPs are sold on Russian forums. Actors like FirstVPN offer a variety of VPN configurations with servers available in 24 different countries for untraceable network activity. These different autonomous services comprise a sort of dark web ISP, upon which the criminal underground is built.

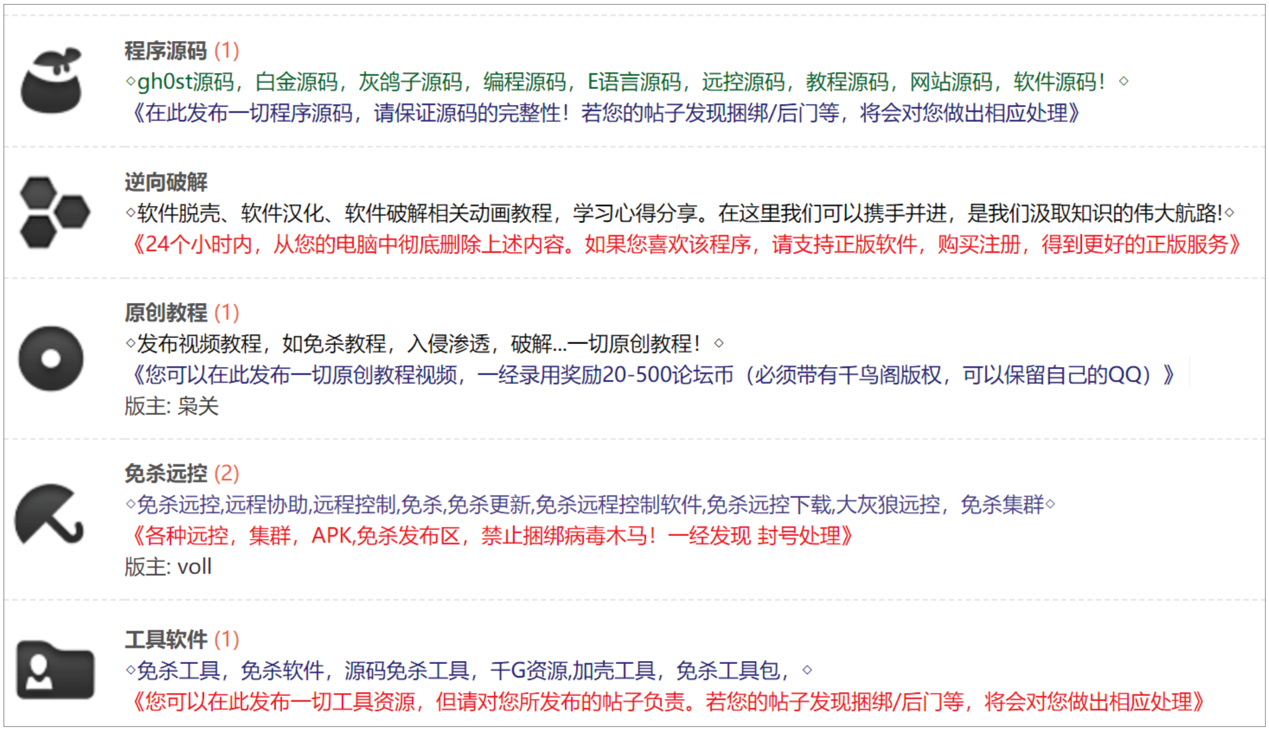
Content in Chinese Underground Forums and Marketplaces

Malware

Common categories within Chinese malware forums include DDoS tools, remote access trojans, antivirus evasion techniques, and penetration testing. Certain forums will also contain sections for cracked software and will have areas for individuals to hire hackers. In addition to selling malware and other tools, individuals will share programming and hacking tutorials on these same forums, occasionally offering or asking for teaching or mentorship services.

Many posts on malware and tooling on the clear web usually use code words or state that the use of these tools is only for "research purposes."

Many lower-tier or open Chinese forums contain advertisements either for malware created by foreign vendors, or open source tools. However, the same forums often also contain malware unique to these Chinese communities. Much of this malware originates from newer hackers who wish to receive criticism of malware they write themselves and usually only have access to lower-level forums. Forum posts under the original advertisement will often contain reviews of custom malware and suggestions on how the malware author can improve. Because of this, individuals will often release multiple builds of their product, similar to users on Russian forums. However, unlike their Russian counterparts, many Chinese malware authors will offer up their source code for a small fee in order to receive feedback from other members to incorporate into newer editions. Cracked software is also often advertised on Chinese forums and is usually tailored to the East Asian market. For example, Xunlei Download Manager, YangCong Math, and the Baidu Wangpan cloud service are all products primarily consumed by Chinese speakers, and cracked versions of their software are readily found on underground Chinese forums.



程序源码 (1)
◇gh0st源码，白金源码，灰鸽子源码，编程源码，E语言源码，远控源码，教程源码，网站源码，软件源码！◇
《在此发布一切程序源码，请保证源码的完整性！若您的帖子发现捆绑/后门等，将会对您做出相应处理》

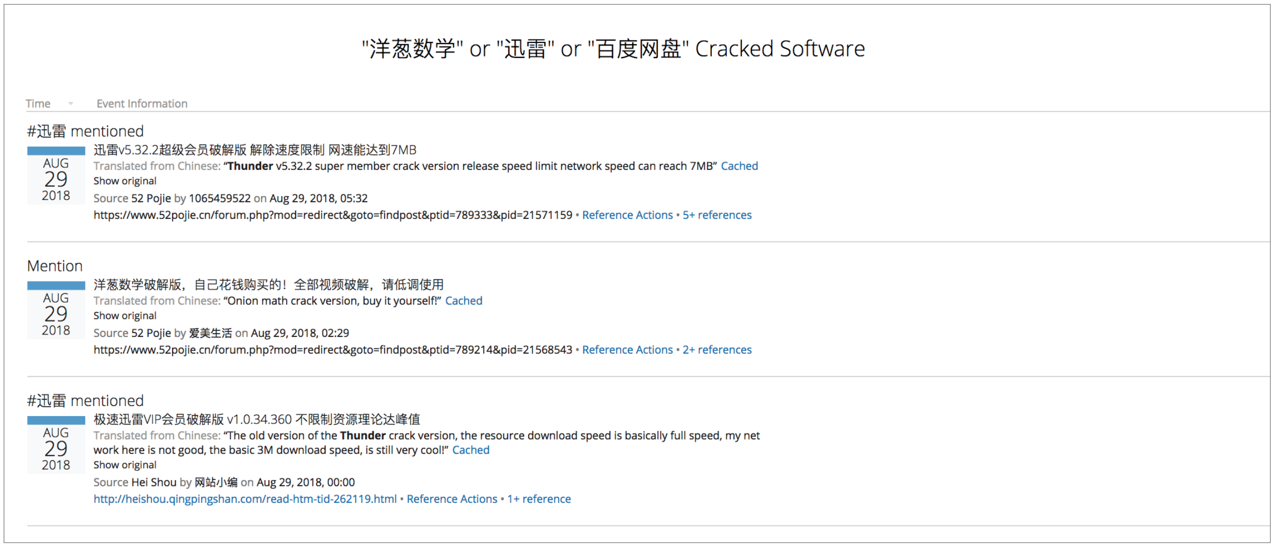
逆向破解
◇软件脱壳、软件汉化、软件破解相关动画教程，学习心得分享。在这里我们可以携手并进，是我们汲取知识的伟大航路!◇
《24个小时内，从您的电脑中彻底删除上述内容。如果您喜欢该程序，请支持正版软件，购买注册，得到更好的正版服务》

原创教程 (1)
◇发布视频教程，如免杀教程，入侵渗透，破解...一切原创教程！◇
《您可以在此发布一切原创教程视频，一经录用奖励20-500论坛币（必须带有千鸟阁版权，可以保留自己的QQ）》
版主: 枭关

免杀远控 (2)
◇免杀远控,远程协助,远程控制,免杀,免杀更新,免杀远程控制软件,免杀远控下载,大灰狼远控，免杀集群◇
《各种远控，集群，APK,免杀发布区，禁止捆绑病毒木马！一经发现 封号处理》
版主: voll

工具软件 (1)
◇免杀工具，免杀软件，源码免杀工具，千G资源,加壳工具，免杀工具包，◇
《您可以在此发布一切工具资源，但请对您所发布的帖子负责。若您的帖子发现捆绑/后门等，将会对您做出相应处理》

Forum categories including source code sharing, software cracking, tools and software, and remote access trojans.



"洋葱数学" or "迅雷" or "百度网盘" Cracked Software

#迅雷 mentioned

AUG 29 2018

迅雷v5.32.2超级会员破解版 解除速度限制 网速能达到7MB

Translated from Chinese: "**Thunder** v5.32.2 super member crack version release speed limit network speed can reach 7MB" Cached

Show original

Source 52 Pojie by 1065459522 on Aug 29, 2018, 05:32

https://www.52pojie.cn/forum.php?mod=redirect&goto=findpost&ptid=789333&pid=21571159 • Reference Actions • 5+ references

Mention

AUG 29 2018

洋葱数学破解版，自己花钱购买的！全部视频破解，请低调使用

Translated from Chinese: "Onion math crack version, buy it yourself!" Cached

Show original

Source 52 Pojie by 爱美生活 on Aug 29, 2018, 02:29

https://www.52pojie.cn/forum.php?mod=redirect&goto=findpost&ptid=789214&pid=21568543 • Reference Actions • 2+ references

#迅雷 mentioned

AUG 29 2018

极速迅雷VIP会员破解版 v1.0.34.360 不限制资源理论达峰值

Translated from Chinese: "The old version of the **Thunder** crack version, the resource download speed is basically full speed, my net work here is not good, the basic 3M download speed, is still very cool!" Cached

Show original

Source Hei Shou by 网站小编 on Aug 29, 2018, 00:00

http://heishou.qingpingshan.com/read-htm-tid-262119.html • Reference Actions • 1+ reference

Mentions of cracked software on forums collected by Recorded Future.

Fraud

While Chinese forums will advertise credit card data and personal information belonging to international users of large multinational corporations, many posts will also contain equal amounts of data belonging to China's unique domestic technology industry. For example, Taobao and Alipay accounts are almost as prevalent as a set of Visa card numbers on certain forums. Most data belonging to these companies consist of East Asian user accounts.

Furthermore, some of this data is only found on Chinese forums, as is the case of a data dump from 51job, Inc. from June 2018. The dump of 2.45 million accounts from the major Chinese job board and provider of integrated human resource services was found by Recorded Future on DeepWebChinese on June 14, 2018. Recorded Future did not detect any other reference to the data dump on any non-Chinese forums. Similarly, Chinese delivery service SF Express also suffered a data breach in July 2018, the content of which has only shown up on Chinese dark web marketplaces as of late August 2018.

Recorded Future assesses with medium confidence that domestic data dumps are not shared beyond domestic Chinese marketplaces due to linguistic and cultural barriers. Not only is there little language crossover between forums, but the act of taking advantage of a Chinese account or personal information requires knowledge of Chinese services. China's technology industry is largely tailored to its domestic market with services and functionality that are distinct from their international competitors. For this reason, Chinese accounts are primarily used and understood by native Chinese-speaking individuals.

Aside from providing opportunities to make money through cybercrime and identity theft, Chinese vendors will advertise forged documents for sale, most of which are tailored to a Chinese audience. Foreign diploma forgeries are incredibly popular. Paste sites and forums of all languages show Chinese advertisements for diploma creation services to fool family and friends. Many vendors even claim that their diplomas fool state-owned corporations, which check credentials through the Chinese Ministry of Education. Other common forgery services found include forged foreign passports and Chinese business licenses. Vendors play into the concept of "mian-zi" in China to attract clientele by claiming that these diplomas, passports, and business licenses will provide better career opportunities and respect from family members. Like Chinese hackers, Chinese fraudsters will also openly sell their tools and tutorials alongside their wares.

What Is Mian-Zi?

The concept of "mian-zi," or "face," can be described as gaining and retaining respect or prestige from peers. Much of China's culture revolves around this concept, especially when pertaining to family and business. "Losing face" can be such a fear for individuals in China that they would rather deceive others than be honest about their shortcomings. For example, many women going back to their hometowns over Chinese New Year would prefer to rent fake boyfriends to show off to their parents rather than admit that they are single, and young Chinese businessmen have realized that purchasing a fake diploma is an easy way to beef up a resume before looking for a job.

Miscellaneous: Weapons, Pornography, VPNs

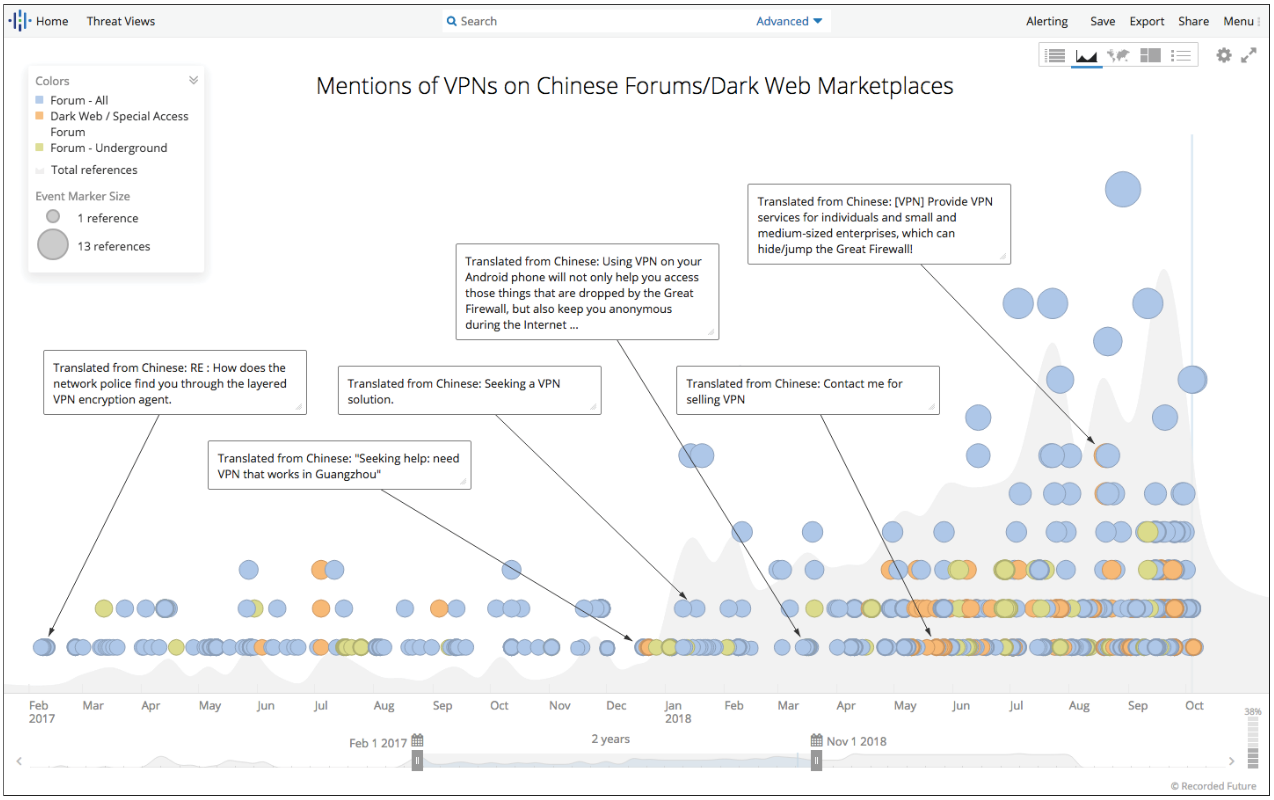
Compared to other hacker forums, Chinese marketplaces advertise a wide variety of miscellaneous wares that are uniquely tailored to Chinese and other East Asian buyers. Although the possession of many of these items are completely legal in other countries, they are illegal in mainland China.

For example, only a small amount of the pornographic content shared in Chinese marketplaces would be considered illegal outside of China. However, the Chinese Communist Party considers all pornography to be a form of "illegal publication," and its General Administration of Press and Publications (GAPP) has attempted to shut down pornography sites since the early 2000s. As such, online pornography vendors have evolved from blatant advertising to using internet slang (the terms "welfare"[10] or "getting on a car"[11] are both common terms for explicit content) and have moved largely from open sites to live-streaming applications and underground forums.

As for weaponry, large knives are commonly found on Chinese dark web marketplaces. This is likely the result of national regulation controlling the sale of knives with blades larger than 5.9 inches, due to knife attacks within the country in 2008, 2011, and 2014 attributed to Uighur separatists.

Although the sale of VPNs is not a uniquely Chinese forum characteristic, the massive number of VPNs for sale on Chinese forums is notable. Mentions of VPN access shared or sold on Chinese underground forums have steadily increased since January 2017, when the Ministry of Industry and Information Technology announced that it now requires VPN providers to be licensed by Chinese officials. The activity rose even more rapidly once China's official ban against VPNs came into effect in March 2018

[10] 福利: Welfare/material comforts; slang for explicit content.
[11] 上车: Getting on a car; slang for sharing explicit content.



Translated from Chinese: RE : How does the network police find you through the layered VPN encryption agent.

Translated from Chinese: "Seeking help: need VPN that works in Guangzhou"

Translated from Chinese: Seeking a VPN solution.

Translated from Chinese: Using VPN on your Android phone will not only help you access those things that are dropped by the Great Firewall, but also keep you anonymous during the Internet ...

Translated from Chinese: Contact me for selling VPN

Translated from Chinese: [VPN] Provide VPN services for individuals and small and medium-sized enterprises, which can hide/jump the Great Firewall!

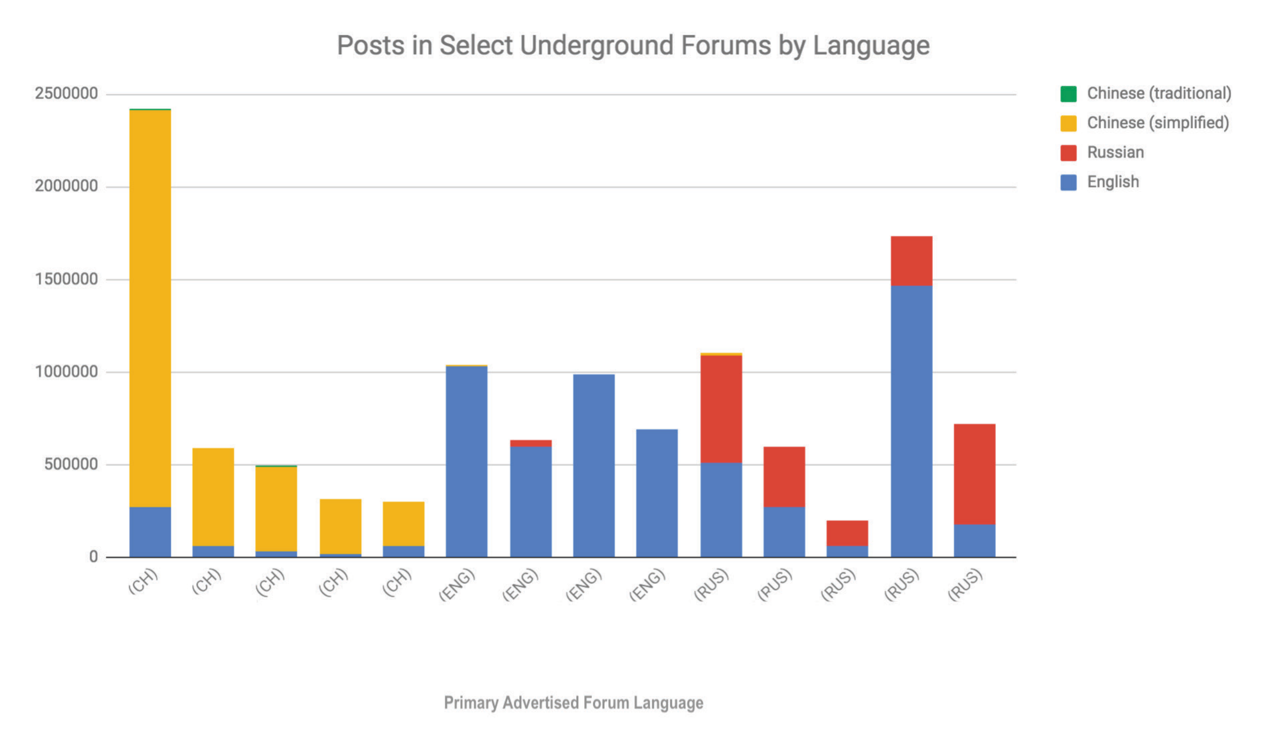
Mentions of VPNs on Chinese forums and dark web marketplaces in Recorded Future.

Interactions Between Chinese and Russian Hackers in Forums

Analysis of select underground forums in Recorded Future demonstrates that Russian forums consist of primarily English and Russian posts with some Chinese overlap. The Chinese posts indicate that Chinese vendors are communicating with Chinese buyers on foreign forums. Additionally, many Chinese posts within Russian or English forums are fraud services tailored to Chinese audiences, like the fake diploma sales mentioned above.

In contrast, Chinese forums consist almost entirely of Chinese language posts, with most English posts on the forums consisting of numbers, code, or simple words. Thus, it is probable that while some Chinese vendors and buyers are on Russian and English forums, very few non-Chinese vendors advertise on Chinese forums. The lack of Russian or English speakers on Chinese forums could be due to a language barrier that exists between Chinese and Russian hackers. Chinese is among one of the hardest languages to learn and only a handful of Russians speak foreign languages at all.

More likely, however, is that the abundance of Russian and English language hacking forums eliminate the need for actors fluent in these languages to search for other forums. These two points would also explain the lack of Chinese malware or data dumps on non-Chinese forums. Because non-Chinese speakers do not use both sets of forums, products that originate on Chinese forums are less frequently resold on foreign forums, if at all. On the other hand, even the small presence of Chinese speakers on non-Chinese forums indicates that Chinese vendors are attempting to decrease their exposure to domestic monitoring and government intervention, while increasing their exposure to buyers posting in foreign marketplaces to ensure they stay in business. If so, this may be a result of the Chinese government's efforts to censor and shut down Chinese forums.



Breakdown of select forums by post language. Source: Recorded Future data.

Outlook

The hacker cultures of China and Russia each have their own unique genesis and have evolved to take advantage of their respective regional circumstances. Understanding the differences within these communities is essential to grasping the respective threats they currently pose and the manner in which these threats may evolve.

Recorded Future assesses with high confidence that the Russian underground will follow the money above all else. Predominantly, these forums have catered to the former Soviet Bloc, but they also have a unique appeal to the international community, as the databases and credit cards sold on them come from victims throughout the world. The exploit kits and bulletproof hosting are open to most anyone with enough Bitcoin. In fact, a number of sales threads on Russian forums are posted in both English and Russian, demonstrating a willingness to expand into other markets. This cross-cultural endeavor is reminiscent of the original fraudster forums and could once again bring the English-speaking hacker communities closer to their Russian comrades. Anyone with enough background in English — a mandatory language to study in China — could find their way into some of these Russian forums and access the extensive criminal arsenal therein. This may result in the exchange of tactics and tools across English, Chinese, and Russian-speaking criminal groups, whose target bases will suffer from potentially new methods of attack.

The members of the Russian-language cyber underground pose a global threat due to their sophistication and diverse criminal operations. Regardless of their location, every financial institution, social network, and ISP should take note that they and their customers are or could be a target, and ensure that their systems are continually patched against commonly known vulnerabilities.

Recorded Future also assesses with medium confidence that China's determination to shut down Tor and VPN access to its citizens in a crusade toward a "clean and righteous internet" will cause Chinese markets and hacker forums to shut down. Increasing numbers of Chinese dark web vendors will peddle their wares on foreign sites as a result, thereby increasing foreign access to previously unique regional malware and hard-to-get data. If no drift occurs and the Chinese underground forums do not shut down while China tightens its noose on online anonymity, we assess that the Chinese government implicitly accepts domestic cybercrime under a certain threshold.

For now, companies doing business in China or the wider East Asian region should monitor Chinese hacking forums and marketplaces for credential leaks and operations targeting company infrastructure, due to the variety of East Asia-specific data, specifically on these sets of forums. Additionally, companies with offices within East Asia should ensure that their infrastructure is secured against malware developed within Chinese forums, and monitor politically sensitive regional events that might spur Chinese patriotic hacktivism.

About Recorded Future