THE DARK SIDE OF ASIA
AN INSIDE LOOK INTO ASIA’S GROWING UNDERGROUND WORLD
INTRODUCTION
The “Dark Web” is a growing buzzword in the world of cybersecurity and general technology. Many people have heard of it, while some might even have the courage to install the TOR browser and visit the dark web for themselves. Whether you’ve visited the dark web or not, it’s important to understand how it’s used by cybercriminals and different underground communities so that you can leverage it as a source of threat intelligence.

As the dark web has grown in size and usage, various regions of the world have developed their own dark web communities and “codes of conduct” that can differ quite dramatically. In addition, each government has its own laws and viewpoints towards illegal cyber activity, which can either hinder or enable how cybercriminals use the dark web (or other networks, as we’ll discuss later) in that region.

We often tend to associate hacking activities to Russian, North Korean or other English-speaking cyber groups. However, over the past few years, we’ve seen an increase in dark web and cyber activity across Asia. This new rise of the underground Asian Internet has presented companies and threat hunters across the globe with a number of new challenges. Finding cyber threat hunters who are fluent in the local language is a challenge alone. However, threat hunters also need to be intimately familiar with the dark web slang and rules of engagement of that region, so they can effectively blend in and perform reconnaissance.

Lastly, it can be incredibly difficult to gain access to the right secret forums and networks. As we’ll discuss later with the Chinese Internet network, many hackers are not even using the dark web or openly-accessible anonymous networks, because they use networks that are kept private and protected by their governments. This leads to a number of additional challenges threat hunters must work around.

In this research report, we uncover the Dark Side of Asia to provide you with an inside look into key trends, laws, motivations and threat actors of the increasingly threatening Asian Internet community.

Dark Web Cultural Differences
When you visit another country, you often need to adjust to new cultural differences and norms. The same goes for visiting other countries’ underground Internet communities. Each country has their own “dark web culture” that you must adhere to and laws that govern them. Being fluent in the language is not enough, you must know the jargon and rules of engagement for each country or else you’ll be kicked out.

Because each dark web has its own cultural and legal differences, it can be difficult to perform reconnaissance across their communities and forums. Understanding these differences is key to developing sources and gathering intelligence without being suspected by the other users.

In addition, it can be difficult to find VPNs and access points to these various web communities (we’ll get into this more later on), so maintaining your cover is key.
THE POLITE, INNOCENT, ENVIRONMENTALLY-FRIENDLY COUSIN OF THE DARK WEB WE KNOW
BACKGROUND

The origin of the dark web scene in Japan can probably be traced back to late 2012 or the beginning of 2013. While many people consider illegal activity to be the primary use for the dark web, Japan perceives the dark web differently. Many Japanese users view it as an alternate universe where they can express themselves and have harmless discussions, just behind the mask of an anonymous avatar. It is not uncommon to see diaries and blogs on the Japanese dark web.

It’s also worth noting that avatars and notoriety are much less important in the Japanese dark web compared to the Western dark web. Japanese users tend to care more about getting content online, rather than taking credit for attacks or gaining recognition among the community.

Many Japanese dark web users communicate through Bulletin Board Systems (BBS), which allow users to disseminate content quickly and anonymously. Some users leverage forums and private chat platforms to communicate, but those are still quite scarce as most Japanese users prefer the BBS platform.

While the Japanese dark web can be completely innocent at times, there are still many illegal activities that take place.
THE LANDSCAPE OF THE JAPANESE DARK WEB

The Japanese dark web offers many different goods and services, but the two most common commodities are:

1. Narcotics
2. Child pornography

While this is not vastly different from other dark webs, there are some key differences in how vendors sell and engage buyers for these goods.

Quite a few Japanese drug dealers allow prospective buyers to sample their product and return it free-of-charge if they’re not satisfied (you’d be hard-pressed to find that type of service from other drug dealers, either online or in-person). They also tend to be much more respectful than their Western counterparts, which you can see based on the distinct differences in casual Japanese compared to more polite and formal Japanese.

Below are some examples of common posts or goods you can find across Japanese black market forums. You can also see a few discussions on carding and credit card dumps.
There are also invitations to form hacking groups:

*Image 6: invitation from Japanese threat actor to take a part in a Japanese hacking group.*

*Image 7: A screenshot from a website that invites Japanese users to sell state and military secrets. (This may very well be a Chinese or North Korean that is attempting to gather intelligence for some attack on or operation in Japan).*
LAWS & POLICIES

Legislation in Japan is very supportive of acting against cyberattacks. Japan is one of the first countries worldwide to have specifically outlawed malware creation and distribution, referencing them directly in legislation and imposing prison sentences for offenders. Arrests have already been made on those charges, and more will probably follow. In addition, networking crimes have consistently increased in Japan since the early 2000’s.

However, Japan also suffers from some significant constitutional challenges that prevent it from being able to proactively respond to cyber threats (particularly state-sponsored ones).

• **Article 9 of the Japanese Constitution** - This article completely outlaws war as a means of settling disputes. This means that Japan is unable to initiate cyberattacks against other states, even if they are completely pre-emptive in nature.

• **Article 21 of the Japanese Constitution** - This article guarantees the integrity and secrecy of the various means of communication. This means authorities are (usually) unable to shut down communication infrastructure (even in the case of an ongoing attack), or utilize wiretaps to track cybercriminals.

This situation makes it extremely difficult for Japanese authorities to obstruct criminal activity on the dark web and establish legal grounds for investigative operations or preventive action. For instance, they are unable to seize websites in their respective territories, unlike US and European authorities. As a result, Japanese cybercriminals have more room to maneuver and don’t have to worry about their dark web operations being interrupted.

As such, the criminal cyber climate in Japan tends to be unrestricted by the state’s institutions.


### CYBER HACKTIVISM IN JAPAN

Hacktivism is particularly prevalent in Japan. Japanese hacktivists are mostly concerned with environmental issues, but overall can be divided into four categories:

**Denuclearization (OpFukushima & OpNuke):** Hacktivists constantly reference the aftermath of the Fukushima crisis. Hacking groups often publish target lists and call for DDoS and defacement attacks on websites that are associated with managing this crisis. This hacktivist campaign has gained even more prominence recently, because the storage capacity for the facility’s contaminated water is approaching the limit, and the government is planning to slowly dump the excess into the Pacific Ocean.

**Treatment of Animals and the Environment (OpGreenRights & OpKillingBay):** Hacktivists often protest how Japanese hunters treat whales and dolphins, pointing to the sheer cruelty the animals experience. This protesting is usually done by hacking fishing companies’ websites or public accounts and posting extremely graphic images. Hacktivists usual target groups in Taiji, a fishing village in southern Japan that is infamous for its whaling practices. In December 2015, hacktivists took the Japanese prime minister’s website down in protest over Japan’s whaling operations. DDoS attacks on other government offices and infrastructure operators have also been recorded.

**Political Hacktivism:** This is less common than the previous two motives, but is still seen from time to time. Some Japanese hackers sympathize with the political situation in other countries, as seen in the attack carried out in Image 9 to the right. Furthermore, Anonymous in Japan are very concerned with the rise of ISIS and are committed to taking it down.

**Miscellaneous Causes:** There are many other examples of hacktivism in Japan, particularly focused on environmental issues. For example, in the beginning of 2018, hacktivists accused the Japanese government of cutting down forests to supply lumber for the construction of the 2020 Olympic facilities.
JAPAN’S THREAT ACTORS

0chiaki

Born in 1997, 0chiaki is the writer of Japan’s first ransomware: Karansomware. Before this attack, Japanese Internet users were mostly just collateral damage from previous ransomware attacks, but Karansomware was the first ransomware with the specific intention of attacking Japanese users.

0chiaki used a malicious Adobe Flash update request to get users to download and install the ransomware onto their computers. Once installed, it encrypted the user’s files and demanded that they pay ¥40,000-300,000 to decrypt them.

0chiaki’s first run-in with the law was when he was 15 and was arrested for hacking a bulletin board. Since he was a minor, he was sent to a juvenile facility instead of prison. When he was 18, he was arrested again, this time for creating Karansomware and stealing his victims’ credit card details. He was sentenced to a year and a half in prison.

After his release from prison in 2016, he started a blog where he discusses various issues relating to cyber security, web anonymity and Bitcoin.

Image 11: Karansomware’s lock screen
**Darkness Onion-kun**

Darkness Onion is a hacker that for the past few years has actively been carrying out DDoS attacks on various websites. In August 2017, they opened a Twitter account which was used as their main method of publishing their “work”. Almost 11,000 users followed their profile, a great deal of whom interacted daily with Darkness Onion.

Darkness Onion was somewhat unusual in their behavior, because although Japanese hackers typically communicate through Twitter, Darkness Onion was purposely attracting a great deal of attention to themselves. They held contests to see which site they’d target next and when they’d stop their DDoS attacks. When an online Japanese magazine picked up the story and wrote about them, they were thrilled to have had the recognition.

Things seemed to be going quite well for them, but all of that came to an end on April 30, 2018 when for seemingly no reason, they tweeted they would no longer be uploading new content to the profile. It remains to be seen whether they will make a comeback or if the profile will stay dormant.

*Image 12: Darkness Onion-kun Twitter Page*
RED IS THE NEW DARK (WEB)
BACKGROUND

The Internet arrived in China in 1994. By the year 2000, there were about 22.5 million Internet users within China, which was only about 1.8% of this huge country’s population. By 2018, China’s Internet population reached more than 772 million users, with a penetration rate of 55.8%, exceeding the global average of 51.7%.

Chu Tianbi, the writer of Chinese Hacker History, states that hacking in China started in 1994, when the Internet just arrived in the country and its citizens became users. However, in 1997, there were only 7 elementary hacker webpages in China, most of which were just copying information from foreign websites.

Throughout these early years, Chinese hackers were very unsophisticated, but over the past 10 years, the hacker culture has evolved tremendously. Chinese hackers have become highly equipped, mature, advanced and well-experienced.

THE LANDSCAPE OF THE CHINESE UNDERGROUND INTERNET

Government Influence

Unlike most other countries, China uses a government-controlled Internet network that allows the government to monitor and control all access, activity and users across this network, as well as blocking the access to some foreign webpages. This has created an interesting dynamic amongst Chinese Netizens (Internet Users) and makes it particularly difficult to conduct threat reconnaissance against Chinese hackers.

The relationship between the Chinese government and Chinese hackers is quite interesting. As long as the hackers are “helping” the Chinese government’s interest and agenda, they typically cooperate with one another. However, when a Chinese hacker’s interests do conflict with national interests, the government will do anything and everything to restrict, censor and even prosecute the hacker. The government does attempt to fight against Chinese cybercriminals, for example shutting down their websites and making arrests when they can, but due to the sheer number of websites and users in China, even the monitoring and censoring activity being done by the government cannot stop all cybercriminal activity on the Chinese web. For this reason, users can find a wide variety of goods across the Chinese underground communities (more on this in the next section).

Dark Web vs. Clear Web Usage

While in other countries cyber criminals would usually turn to the deep and dark web in order to offer their services or products, the Chinese are more active on the clear net because the government limits access to the dark web. In addition, cybercriminals can reach a greater pool of buyers on the clear Chinese Internet and achieve higher profits. Obviously, this makes it more risky for the seller, so Chinese cyber criminals use special “jargon” or “code names” to avoid government censors and crackdowns. While there are tens of thousands of dark websites in Russain and English, the number of Chinese websites is rather small. Moreover, some of the webpages originate from Hong Kong and Taiwan.

Public forums such as the Chinese Deep Web are typically used by ordinary people and unexperienced hackers that are trying to improve their skills. These forums are very active, but the number of users is very small in comparison to the overall Chinese population.
Communication Channels
Using the different websites and social media platforms on the Chinese web, vendors publish their products and services in order to find potential buyers. One of the most common channels used is QQ, which is a popular social media network that provides communication tools such as QQ groups, QQ forums and private chatrooms. Other common platforms include Baidu Paste Bar³ (Baidu Tieba), which is a communication platform as part of the Baidu search engine. Another platform is Baidu Knows⁴ (Baidu Zhidao), which acts as a forum where users can publish threads and questions for others to answer. Many people use this platform to ask where they can get an illegal product or service, and sellers can respond.

Cryptocurrency Use
Another big difference for Chinese black markets is the use of cryptocurrency (or lack thereof). While in other countries cyber criminals usually use popular cryptocurrencies, like Bitcoin, most Chinese black markets use RMB (CNY), the Chinese currency.
LAWS & POLICIES

The Golden Shield Project
In light of the citizens’ online protest, in 1998 the Chinese government started the Golden Shield Project (jindun gongcheng), which is the Chinese nationwide network-security constructional project. The Great Firewall of China, a subproject of the Golden Shield, is a censorship and surveillance project that regulates the Internet and blocks access to inconvenient data. The goal behind the project was to encourage “the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work.” By the year 2008 the project was fully completed.

Internet censorship is enforced through shutting down websites, blocking specific search terms, and slowing down connectivity for users that are considered problematic by government censors. As of May 2018, more than 8,000 domain names are blocked in China.

Internet Sovereignty & The Chinese Communist Party
The Chinese Communist Party extends its assertion of national sovereignty to the cyberspace and views the Internet as “Internet Sovereignty”. According to this notion, the Internet inside China is part of the country’s sovereignty and should be governed by the country, as the country has a right to regulate the stream of information.

Internet censorship in China is based on more than 60 regulations that have been created by the Chinese government. In May 2010, the Chinese government issued its first white paper on the Internet that focused on the concept of “Internet Sovereignty”, requiring all Internet users in China to abide by the Chinese laws and regulations. In June 2017, the first Chinese cyber security law took effect. This law re-affirmed China’s commitment to controlling what technology is used within the country and how it collects information.

VPN & Access Crackdown
VPN (virtual private network) services have become the most popular way for Chinese netizens to circumvent the Great Firewall of China. Throughout the years, the Chinese authorities have been trying to block access to VPN services inside the country. In July 2017, the Chinese government started the most severe crackdown on VPN usage in China by requiring the three big Chinese telecommunication networks (China Mobile, China Telecom and China Unicom) to ban individuals’ access to VPNs by February 1, 2018. In the same month, Apple removed VPN services from the China App Store.

Chinese Government Mandates
In September 2017, WeChat, the Chinese messaging app owned by Tencent, released an update informing users that all private customer information will be disclosed to authorities in China. It was the first time a company in China had confirmed sharing information with the government in order to comply with the laws and regulations.

In August 2017, the Cyberspace Administration of China published rules that declared that Internet forum providers were responsible for ensuring that their users are registered using their real names, which the providers must also verify. Also, Internet service providers were obliged to screen comments and immediately report any illegal comments to the authorities.

In practice, this online ecosphere, which is heavily monitored and censored, is the reason individuals in China have become very technologically knowledgeable, as VPN, SSH and proxy servers are a necessity for them to view censored information.
GOODS & SERVICES ACROSS THE CHINESE INTERNET

The Chinese are known to have a wide variety of materials and services available across their dark web. This is mostly due to the Chinese government selectively enforcing laws against cybercriminals. Here are some of the most common goods and terminology used across the Chinese Internet.

Drugs / Narcotics: Many Chinese drug vendors began to understand that operating using the Chinese web might be too risky. Therefore, around 2014 they started to move into dark web black markets. Some use Chinese websites like Mushroom, which offers many types and different brands of drugs. Others are using the Western black markets, such as Dream Market. If you were to search Dream Market, you’d see hundreds of drugs listed by Chinese vendors who sell from the Chinese Mainland.

Forged Documents: Some vendors offer fake passports, I.D cards, driver’s licenses, Social Security cards, university diplomas and more. You can also find services for changing a student’s university or high school GPA. To find diplomas for sale, you’d use the search term “Banli Xueji”, which literally means to handle educational background. A few hacking groups promote those services using videos on YouTube.

Data for Sale

Commercial Data: Many vendors offer leaked information from different data breaches. This data is either sold as a full database or in parts on the Chinese underground communities. The latest example was the “AcFun6” website, which is a Chinese video-sharing website that was attacked and breached. On June 13, 2018 the company disclosed the attack and admitted that millions of users’ data was compromised. However, Chinese hackers already had AcFun data for sale in a dark web forum on June 8, almost a week before the company’s announcement.

Personal and Private Information: Some vendors offer personal and private information for senior management personnel and executives at various organizations. For example, during our research we found a user in one of the dark web forums offering information about 13 executives at TCL corporation, which is a Chinese multinational electronics company with yearly revenues of over $16 billion.
Bank Account and Credit Card Information: Just like any black market, financial information is a popular “good” across Chinese black markets. Credit card and bank account information are called “Material” in Chinese (Liao). “Material washing men” (Xi Liao Ren) are the people that sell information on the underground markets. Material master (Liao Zhu) are the criminals who steal and sell bank account information. Envelope (Xin Feng) is the term for account and password information. With these search terms and others, you can find an endless supply of stolen bank account credentials and credit card information on the Chinese web.

Doxing: the Chinese term for doxing is “renrou sousuo”, which literally means “human flesh search”. A common doxing service includes researching and publishing personally identifiable information about individuals or organizations.

Cyber Security
DDoS Services and Tools: These are considered to be the most popular products on the Chinese black market. Using the search term “DDoS” (DDoS Gongji Gongju), which means DDoS attack tools, you can find hundreds of results in related hacking groups, dedicated to sharing DDoS tools on Chinese social media platforms (such as WeChat and QQ groups). In addition, using this search term on Google or Baidu will provide many results of companies offering DDoS services on the clear web.

Malware, Exploits and Hacking Tools: Malware and exploits are products that are not easy for a regular user to acquire. What usually happens is QQ hacking group masters (which go by different names like Qunzhu, Chezhu, Daxia) would buy malwares and exploits directly from a malware writer. They will later sell it to professional and novice hackers on their private groups. On the other hand, hacking tools are found easily across the clear net. We found a variety of hacking tools for sale during our research across different groups, including SQL injections, tools for remote control, PowerShell’s and guides.
**Hacking-as-a-Service:** Individual hackers and hacking groups offer hacking services, including social media and bank account takeovers, DDoS, defacement, Doxing, website hacking, writing zero-day exploits, source code stealing, spam services, and phishing. All of these services can be customized to fit specific needs and are offered for sale in QQ groups.

**Hacking Training and Tutorials:** Within the Chinese websites, forums and QQ groups, there are thousands of hacker training services, guides and tutorials for sale.

**Other Services**

**Child Pornography:** Although child pornography is considered to be a severe crime in China, there are many CP websites in the Chinese dark web. In 2016, the Chinese police managed to discover and arrest a few hundred users of the child pornography network in the Chinese dark web. Although the Chinese government doesn’t always enforce their cyber laws, this is an example of them taking action when they feel it’s warranted.

**Human Organs Trade:** During our research, we discovered posts in a few dark web forums and telegram channels from people who offered human organs for sale.
CHINESE INTERNET MOTIVATIONS AND USES

During our research, we observed that Chinese cyber groups are using the Internet for several main activities (i.e. motivations), such as:

- **Nationalism:** The Chinese have a strong sense of national pride, which is one of their noticeable differences when it comes to cyber activity. The Chinese Red Hacker groups believe that hostile activity against Chinese interests should be answered with an appropriate cyber response. It is a sense of nationalism that encourages them to attack back as a way of protecting their country.

- **Cybercrime for Financial Profit:** This activity includes planning, gathering information, looking for exploits, trading carding and other scam methods, all with the goal of making money.

- **Stealing Foreign Intellectual Property:** This is done for the sake of advancing Chinese interests and is sometimes being conducted by state-affiliated hacking groups.

- **Technical Interest:** Some hacking is just done for sport. There are many Chinese forums for computer system experts and cyber researchers.

- **Hacktivism:** These attacks are done to protest against the Chinese government and the Communist Party.

- **Fame:** Chinese hackers are adored by the Chinese people. Hacking in China is portrayed as a lucrative and even respected occupation, and many people aspire to be hackers. As a result, many hackers are hacking for the fame.

- **Opinion Sharing:** Other than hacking, Chinese citizens have used the Internet as a means to manifest their opinions and protest. Studies show that since 1996, the Internet has become a powerful channel for expressing social opinion and protest. Chinese netizens have been constantly seeking new ways to express their thoughts.
**CYBER HACKTIVISM IN CHINA**

Hacktivism in China has been represented by two main types of underground communities:

1. The groups that resist the Communist Party
2. The groups that support Chinese nationalism and patriotism

**Groups Resisting the Communist Party**
The first community is composed of individuals and groups who are against the Chinese Communist Party. Their method for protesting and resisting the Communist party is through cyberattacks against national targets, such as government websites and national telecommunication companies (TV stations, ISPs, cellular operators, etc.). They usually conduct defacement attacks, in which they “push” their messages denouncing the ruling Communist Party. Fangongheike²² is one example of these groups. They have a [webpage](#) and a [Twitter account](#), which has over 14.5K followers. They update their website and Twitter account regularly to show their successful defacement campaigns. In 2015, a software engineer was sentenced to 12 years for committing a defacement attack on one of the popular TV stations in China. As part of the attack, he managed to inject anti-Communist slogans on screen during the famous TV show “The Voice of China”.

**Groups Supporting Chinese Nationalism**
The Nationalism community has become one of the most significant influences behind many Chinese cyber group’s actions. In 1998, riots in Jakarta, Indonesia erupted and targeted the ethnic-Chinese community. For 3 days, the Indonesian mob assaulted, raped and killed people from the Indonesian Sino-community, as they were seen as responsible for the country’s inflation. Chinese hackers were outraged by the events in Jakarta and started gathering in IRC chat rooms. This led to the formation of the first Chinese hacktivist groups. These groups conducted many cyberattacks against the Indonesian government’s websites.

Before the riots in Indonesia, there was only one hacking group in China, called the Green Army. This group, which was formed in 1997 by a hacker named Goodwill, had 3000 members. The riots led to the formation of the term “Red Hacker²⁴” (Hongke, which literally means “red visitor”), as compared to the usual Chinese transliteration of hacker (hēike²⁵, which literally means “Black Guest”, as in black hat). The riots have also led to the formation of the Red Hacker Alliance (Zhongguo hongke lianmeng²⁶). This alliance was a large coalition of smaller groups that combined and had over 80,000 members. Before the formation of this group, there were only individual hackers and very small cyber groups that were operating in China.

In 1999, during the Kosovo conflict, the U.S. accidently bombed the Chinese embassy in Belgrade, killing 3 Chinese reporters. In response to the attack, members of the Red Hacker Alliance hacked U.S government websites and planted messages against “NATO’s brutal action”.

---

[²² Fangongheike](#)
[²³ Red Hacker](#)
[²⁴ Hongke](#)
[²⁵ hēike](#)
[²⁶ Zhongguo hongke lianmeng](#)
CHINESE HACKERS IN FOREIGN FORUMS

One of our most interesting findings during this research was that Chinese threat actors are using foreign forums to communicate and plan their activities, with a particular emphasis on Russian forums. While searching Russian professional hacking forums and marketplaces on the dark web, we came across many posts written in Chinese. What’s interesting about this is that most Russian forums only allow users to post and communicate in Russian. Any other language is typically taken down, with the exception of Chinese.

It seems the Chinese cybercriminals have opted to turn to foreign forums and websites instead of building their own, and have primarily leaned on the Russian dark websites to do so. Since Russian hackers are known for being highly professional, it is no surprise that Chinese hackers turn to Russian forums in their search for tools and information. However, if they wanted to communicate with Russian hackers, they’d likely write their posts in English, as Chinese is not a commonly understood language. Therefore, the fact that they are writing posts in Chinese means they are likely just using the Russian forum to communicate with other Chinese hackers, rather than communicate with threat actors from Russia or other countries.

THE MOST INFLUENTIAL CHINESE THREAT ACTORS

There are probably hundreds of thousands of Chinese threat actors, including black market vendors, private hacking groups, state-sponsored APT groups, hacktivist cyber groups, individual hackers, scammers and many more. We could write a book on all of the threat actors across China, so we decided to focus on the most influential people of the Chinese cyber scene.

**Goodwell:** His real name is **Gong Wei**. Goodwell is considered to be one of the most influential hackers in China. He is the founder of China’s Green Army, which was the country’s first hacking group. As opposed to other famous Chinese hackers, he has only rarely appeared publicly in the hacking world. Chinese hackers believe that he has contributed greatly to the Chinese hacker community.

**Lion:** His real name is **Lin Yong**. Lion is the founder of the Chinese Red Hacker Alliance, which is considered to be one of the biggest hacking groups in the world. From 1998 to 2001, Lion was one of the leaders of the biggest cyber campaigns, which included attacking multiple private and government targets from Japan, Taiwan and the United States. Nowadays, Lion is not active, but he is still considered to be one of the most influential hackers in China.

**Wan Tao:** His nickname was **Eagle**. He was the founder of the China Eagle Union, a Chinese cyber group that was active from 2000 to 2005. He is considered one of the most experienced hackers in China, leading his group in many cyber campaigns against countries they felt were enemies of China. China Eagle Union got credit for attacking U.S and Japanese government websites and managing to steal confidential emails. Wan Tao shut down Chinese Eagle Union in 2006 and nowadays he runs a security firm.

**Glacier:** His real name is **Huang Xin**. Glacier wrote the Glacier Trojan software, and is considered China’s trojan godfather. In the Sino-US hacking battle, many Chinese hackers used his program to attack.
China and GitHub: A Sticky History

GitHub is a web-based Git repository hosting service that helps developers store and manage their code, as well as share it with others. Over the last five and a half years, they’ve had an interesting relationship with the Chinese government and its netizens.

GitHub was blocked in China using DNS hijacking. The block was lifted after 2 days, after a post on Sina Weibo, which protested the block, was shared over 80,000 times.

GitHub users in China experienced a man-in-the-middle attack. Attackers intercepted traffic between the website and its users in China through a fake SSL certificate.

GitHub suffered a massive distributed denial-of-service (DDoS) attack that lasted 6 days. This attack was believed to have had ties to the Chinese government and used a tool called the Great Canon. The Great Canon is a man-in-the-middle weapon which injects malicious scripts to reroute traffic.

This was when things really became interesting between China and GitHub. During this time, China’s Internet regulators sent an unusual request to GitHub, in which they asked to remove an “issue”, published on March 9, 2016, that suggested president Xi Jinping ordered the Chinese military to murder his half-brother Xi Zhengning. This essay was published by a user named “programthink27”, who has over 8,000 followers. As you can see by the post still being live, GitHub did not comply with China’s request to remove it, but rather, blocked access to this post for users inside China.

On February 28, 2018, GitHub was hit by the largest-ever DDoS attack that peaked at a record 1.35 terabytes.

Many Chinese hackers use GitHub to share hacking tools, malwares, and other malicious programs. However, this does not appear to be the main reason why the Chinese government has repeatedly attacked GitHub. Chinese users are using GitHub to host software that enables routing around China’s Great Firewall. Some of the main GitHub pages that were targeted in the 2015 DDoS attack were repositories that aim to help Chinese citizens circumvent the firewall, which indicates this was a focus and motivation for the Chinese government.

An example of one of these repositories belongs to Greatfire.org, an organization that monitors online censorship in China. Its GitHub repositories include links to individuals who want to access sites that are blocked in China, lists of mirror links for censored websites, and also, software that website owners can use to redirect users to unblocked version of their sites.
SOUTH KOREA
INDONESIA
VIETNAM
SOUTH KOREA
A Growing, English-Speaking Dark Web for Drugs and Stolen Credit Cards

BACKGROUND

The origin of dark web activity in South Korea is estimated to have begun in the mid-2000s. According to security researchers, the number of South Korean users that are active in the dark web is increasing every year.

Most of the South Korean dark web sites are used for illegal activity. These sites are relatively small compared to the number of Internet users in the country, but activity has increased over the past few years.

THE LANDSCAPE OF THE SOUTH KOREAN DARK WEB

The South Korean dark web offers a variety of goods and services, with the most common being:

1. Black markets: The leading products are narcotics and credit card information
2. Child pornography
3. Hidden wikis
4. Hacking forums

South Korea is heavily attacked by its sister from the North. At the moment, there are no significant threat actors that operate out of South Korea.
INDONESIA

A Dark Web for Black Markets and Blackjack

BACKGROUND

It’s believed that the Indonesian dark web began in the late 2000s. In Indonesia, the dark web is not considered to be a “big issue” or critical hacking tool. In fact, most cyber criminals in Indonesia still prefer the surface web and mobile apps, since many common illegal services can be found in regular websites on the clear web.

THE LANDSCAPE OF THE INDONESIAN DARK WEB

Because gambling and casino games are illegal in Indonesia, gambling sites have become increasingly popular, which is one of the primary uses of the dark web in Indonesia. In addition, there are a few hundred dark web sites which offer date rape drugs (known as “Rohypnol”) and child pornography materials. Just like any dark web, the Indonesian dark web offers many commonly found services and products, with the top ones being:

1. Narcotics
2. Child pornography
3. Illegal gambling
4. Hacking forums

Image 28: Indonesian hacking forum and black market for malware and exploits
VIETNAM
A Small, English-Speaking Community to Avoid Government Detection

BACKGROUND
The Internet arrived to Vietnam in the early 2000s. At the beginning, it was primarily used by big companies, government offices and universities, and the government kept strict control over access and content for Vietnamese citizens. As a result, dark web activity started in the late 2000s, where users primarily visited Western dark web sites. Most of the Vietnamese dark web sites are black markets, with the most popular and dominant language being English. The reason for this is that Vietnamese vendors want to reach as many customers as possible and avoid the Vietnamese government and law enforcement agencies.

In June 2017, the Vietnamese government created the Cybersecurity Bill. The goal of this legislation is to allow the government to continue censoring the Internet in Vietnam. This new bill forced many Vietnamese threat actors and black market vendors to the dark web so they could continue with their activities.

THE LANDSCAPE OF THE VIETNAMESE DARK WEB
The Vietnamese dark web only has a few hundred websites, most of which are black markets selling primarily narcotics. Here are some of the most common goods sold across Vietnamese dark web markets:

1. Narcotics
2. Cryptocurrency exchange sites
3. Child pornography

Although the Vietnamese dark web is quite limited, according to TOR statistics the monthly average TOR users during 2017 was about 6500 users.
CONCLUSION

The Asian dark web is relatively small compared to its counterparts in Western countries, such as the United States and Europe. However, this doesn’t mean that it poses less of a threat. In fact, due to the laws and political motivations of these countries, the risk to non-Asian companies is significantly higher.

As a threat hunter and cybersecurity professional, it’s important to know the political and cultural dynamics behind each of these country’s dark web landscapes to understand the motivations and tactics of your adversaries. Knowing their jargon, culture and litigation will help you more effectively conduct threat reconnaissance and protect your organization.

However, this is easier said than done. You need the right tools, expertise and access to conduct this reconnaissance and navigate the differences between these various landscapes. The Chinese underground Internet is totally different from other Asian countries. Because most Chinese cyber activity takes place within the Chinese-controlled Internet, and not on the dark web, it’s difficult to hunt threats and discover cybercriminal organizations from these regions.

The battle against cybercriminals is constantly evolving and never-ending. As technologies and legislation changes, so too must your tactics for threat reconnaissance and digital risk protection. Understanding the tools, tendencies and motivations behind your adversaries will always be a crucial part of how you defend yourself.
**About IntSights**

IntSights is redefining cyber security with the industry’s first and only enterprise threat management platform that transforms tailored threat intelligence into automated security operations. Our groundbreaking data-mining algorithms and unique machine learning capabilities continuously monitor an enterprise’s external digital profile across the surface, deep and dark web, categorize and analyze tens of thousands of threats, and automate the risk remediation lifecycle — streamlining workflows, maximizing resources and securing business operations. This has made IntSights one of the fastest growing cyber security companies in the world. IntSights has offices in Tel Aviv, Amsterdam, New York and Dallas and is backed by Glilot Capital Partners, Blumberg Capital, Blackstone, Tola Capital and Wipro Ventures.

To learn more, visit www.intsights.com.