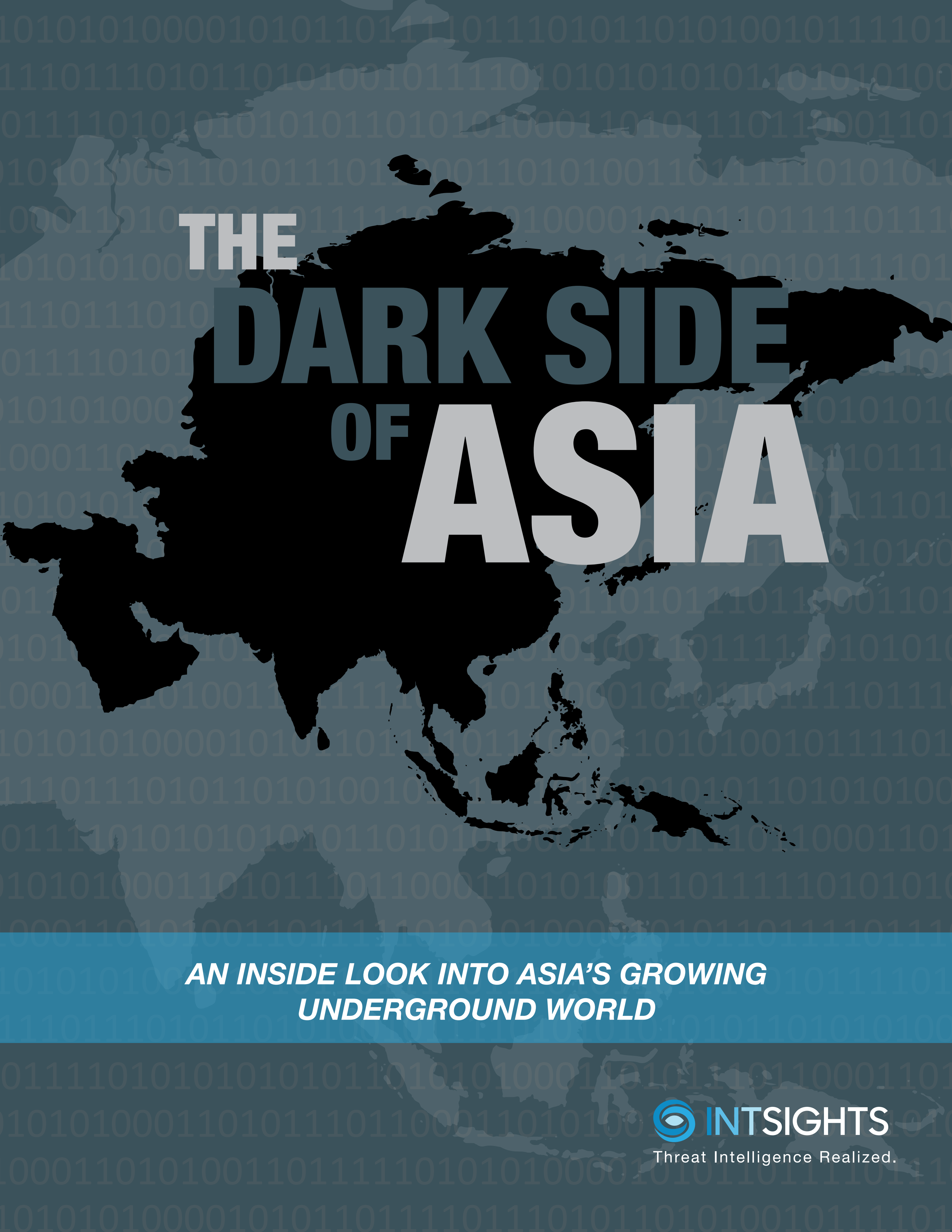


THE DARK SIDE OF ASIA

AN INSIDE LOOK INTO ASIA'S GROWING UNDERGROUND WORLD

INTSIGHTS
Threat Intelligence Realized.

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.

Want to learn more about the how cybercriminals use the Dark Web to plan their attacks?

CLICK HERE TO DOWNLOAD OUR DARK WEB 101 EBOOK.

JAPAN

THE POLITE, INNOCENT, ENVIRONMENTALLY-FRIENDLY COUSIN OF THE DARK WEB WE KNOW

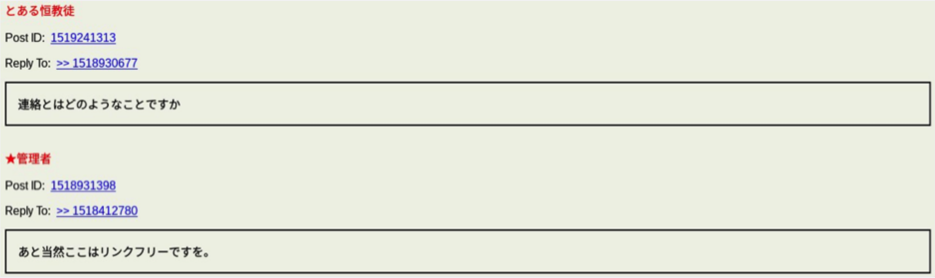
BACKGROUND

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.



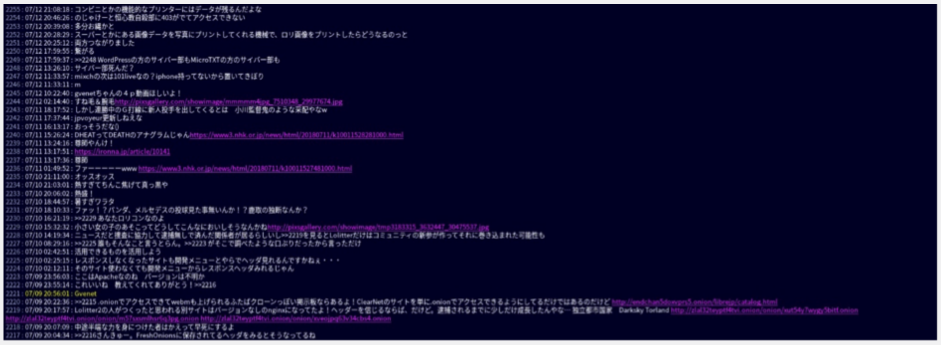
とある恒教徒
Post ID: 1519241313
Reply To: >> 1518930677

連絡とはどのようなことですか

★管理者
Post ID: 1518931398
Reply To: >> 1518412780

あと当然ここはリンクフリーですを。

Image 1: BBS Example



```
2255 : 07/12 21:08:18 : コンビニとかの機能的なプリンターにはデータが残るんだよな
2254 : 07/12 20:46:26 : のじゃけーと恒心教自殺部に403がでてアクセスできない
2253 : 07/12 20:39:08 : 多分お縄かと
2252 : 07/12 20:28:29 : スーパーとかにある画像データを写真にプリントしてくれる機械で、ロリ画像をプリントしたらどうなるのっと
2251 : 07/12 20:25:12 : 両方つながりました
2250 : 07/12 17:59:55 : 繋がる
2249 : 07/12 17:59:37 : >>2248 WordPressの方のサイバー部もMicroTXTの方のサイバー部も
2248 : 07/12 13:26:10 : サイバー部死んだ？
2247 : 07/12 11:33:57 : mixchの次は101liveなの？iphone持ってないから置いてきぼり
2246 : 07/12 11:33:11 : m
2245 : 07/12 10:22:40 : gvenetちゃんの４ｐ動画ほしいよ！
2244 : 07/12 02:14:40 : すね毛＆腕毛http://pixsgallery.com/showimage/mmmmm4jpg_7510348_29977674.jpg
2243 : 07/11 18:17:52 : しかし連勝中のG打線に新人投手を出してくるとは　小川監督鬼のような采配やなw
2242 : 07/11 17:37:44 : jpvoyeur更新しねえな
2241 : 07/11 16:13:17 : おっそうだな()
2240 : 07/11 15:26:24 : DHEATってDEATHのアナグラムじゃんhttps://www3.nhk.or.jp/news/html/20180711/k10011528281000.html
2239 : 07/11 13:24:16 : 草節やんけ！
2238 : 07/11 13:17:51 : https://ironna.jp/article/10141
2237 : 07/11 13:17:36 : 草節
2236 : 07/11 01:49:52 : ファーーーーーwww https://www3.nhk.or.jp/news/html/20180711/k10011527481000.html
2235 : 07/10 21:11:00 : オッスオッス
2234 : 07/10 21:03:01 : 熱すぎてちんこ焦げて真っ黒や
2233 : 07/10 20:06:02 : 熱盛！
2232 : 07/10 18:44:57 : 暑すぎワラタ
2231 : 07/10 18:10:33 : ファッ！？パンダ、メルセデスの投球見た事無いんか！？虚取の独断なんか？
2230 : 07/10 16:21:19 : >>2229 あなたロリコンなのよ
2229 : 07/10 15:32:32 : 小さい女の子のあそこってどうしてこんなにおいしそうなんかねhttp://pixsgallery.com/showimage/tmp3183315_3632447_30475537.jpg
2228 : 07/10 14:19:34 : ニュースだと捜査に協力して逮捕無しで済んだ関係者が居るらしいし>>2219を見るとLolitterだけはコミュニティの新参が作ってそれに巻き込まれた可能性も
2227 : 07/10 08:29:16 : >>2225 誰もそんなこと言うとらん。>>2223 がそこで調べたような口ぶりだったから言っただけ
2226 : 07/10 02:42:51 : 活用できるものを活用しよう
2225 : 07/10 02:25:15 : レスポンスしなくなったサイトも開発メニューとやらでヘッダ見れるんですかねぇ・・・
2224 : 07/10 02:12:11 : そのサイト使わなくても開発メニューからレスポンスヘッダみれるじゃん
2223 : 07/09 23:56:03 : ここはApacheなのね　バージョンは不明か
2222 : 07/09 23:55:14 : これいいね　教えてくれてありがとう！>>2216
2221 : 07/09 20:56:01 : Gvenet
2220 : 07/09 20:22:36 : >>2215 .onionでアクセスできてwebmも上げられるふたばクローンっぽい掲示板ならあるよ！ClearNetのサイトを単に.onionでアクセスできるようにしてるだけではあるのだけど http://endchan5doxvprs5.onion/librejp/catalog.html
2219 : 07/09 20:17:57 : Lolitter2の人がつくったと思われる別サイトはバージョンなしのnginxになってたよ！ヘッダーを信じるならば、だけど。逮捕されるまでに少しだけ成長したんやな…独立都市国家　Darksky Torland http://zlal32teyptf4tvi.onion/onion/xut54y7wygy5bitf.onion
http://zlal32teyptf4tvi.onion/onion/m57sxmmlhsr6q3pg.onion http://zlal32teyptf4tvi.onion/onion/xveojpq63v34cbs4.onion
2218 : 07/09 20:07:09 : 中途半端な力を身につけた者はかえって早死にするよ
2217 : 07/09 20:04:34 : >>2216さんきゅー。FreshOnionsに保存されてるヘッダをみるとそうなってるね
```

Image 2: Japanese Chat System (less common than BBS)

THE LANDSCAPE OF THE JAPANESE DARK WEB

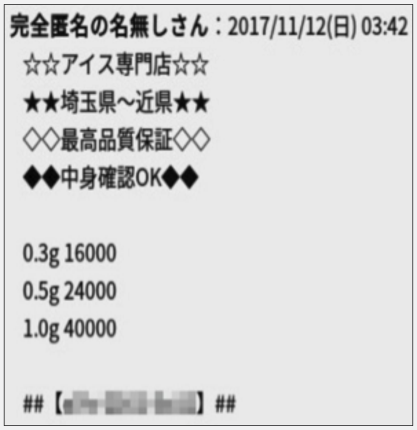
The Japanese dark web offers many different goods and services, but the two most common commodities are:

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.



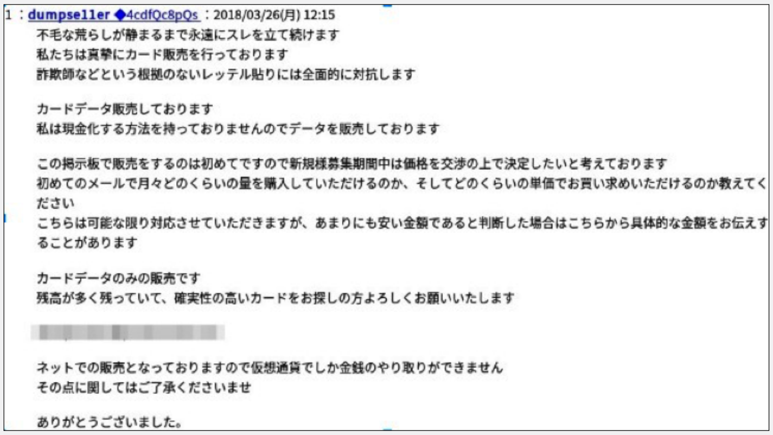
完全匿名の名無しさん：2017/11/12(日) 03:42

☆☆アイス専門店☆☆
★★埼玉県～近県★★
◇◇最高品質保証◇◇
◆◆中身確認OK◆◆

0.3g 16000
0.5g 24000
1.0g 40000

【[redacted]】

Image 3: This user is selling methamphetamines at ¥40,000 per gram. They also mention "testing is OK".



1 ：dumpseller ◆4cdfQc8pQs ：2018/03/26(月) 12:15

不毛な荒らしが静まるまで永遠にスレを立て続けます
私たちは真摯にカード販売を行っております
詐欺師などという根拠のないレッテル貼りには全面的に対抗します

カードデータ販売しております
私は現金化する方法を持っておりませんのでデータを販売しております

この掲示板で販売をするのは初めてですので新規様募集期間中は価格を交渉の上で決定したいと考えております
初めてのメールで月々どのくらいの量を購入していただけるのか、そしてどのくらいの単価でお買い求めいただけるのか教えてください
こちらは可能な限り対応させていただきますが、あまりにも安い金額であると判断した場合はこちらから具体的な金額をお伝えすることがあります

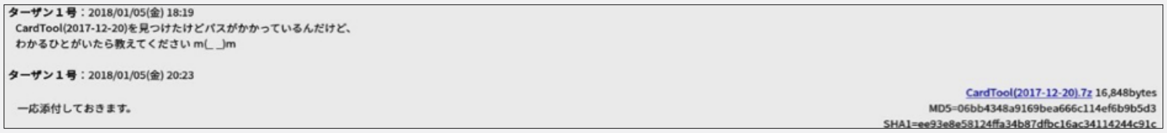
カードデータのみの販売です
残高が多く残っていて、確実性の高いカードをお探しの方よろしくお願いいたします

[redacted]

ネットでの販売となっておりますので仮想通貨でしか金銭のやり取りができません
その点に関してはご了承くださいませ

ありがとうございました。

Image 4: This user is attempting to sell a credit card database. Since it is the first time a database of this sort is being sold on the board, they mention they would like to set the price in accordance with the buyers. This is an example of the polite Japanese mindset on dark web bulletin boards.



ターザン１号：2018/01/05(金) 18:19
CardTool(2017-12-20)を見つけたけどパスがかかっているんだけど、
わかるひとがいたら教えてください m(_ _)m

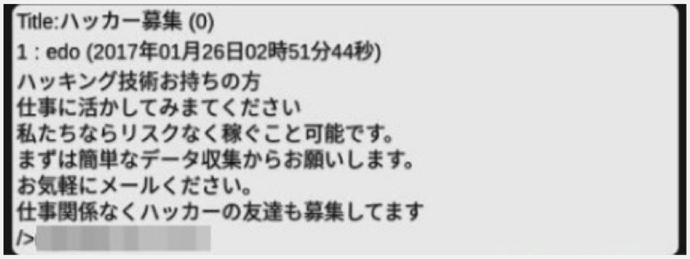
ターザン１号：2018/01/05(金) 20:23

一応添付しておきます。

CardTool(2017-12-20).7z 16,848bytes
MD5=06bb4348a9169bea666c114ef6b9b5d3
SHA1=ee93e8e58124ffa34b87dfbc16ac34114244c91c

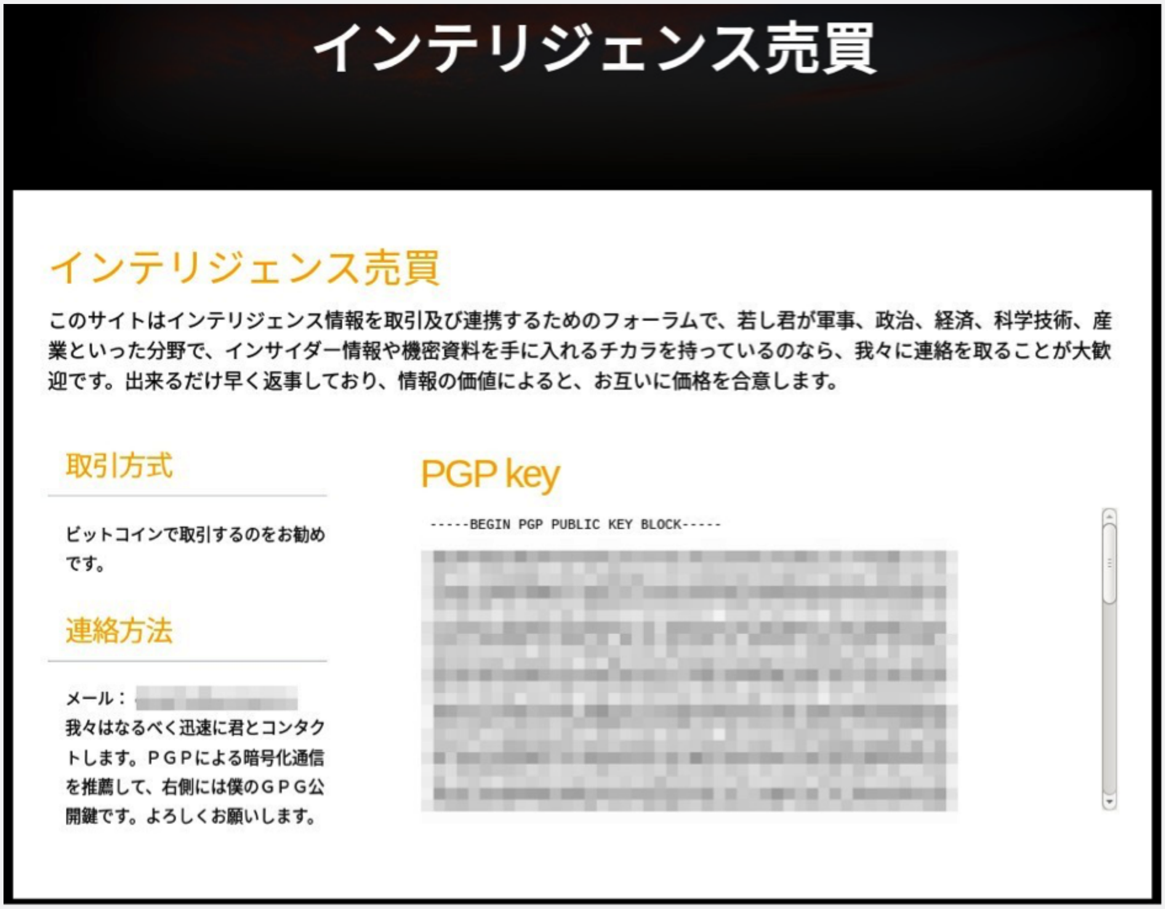
Image 5: Users are discussing carding tools.

There are also invitations to form hacking groups:



Title:ハッカー募集 (0)
1 : edo (2017年01月26日02時51分44秒)
ハッキング技術お持ちの方
仕事に活かしてみまてください
私たちならリスクなく稼ぐこと可能です。
まずは簡単なデータ収集からお願いします。
お気軽にメールください。
仕事関係なくハッカーの友達も募集してます
/>[redacted]

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



インテリジェンス売買

インテリジェンス売買

このサイトはインテリジェンス情報を取引及び連携するためのフォーラムで、若し君が軍事、政治、経済、科学技術、産業といった分野で、インサイダー情報や機密資料を手に入れるチカラを持っているのなら、我々に連絡を取ることが大歓迎です。出来るだけ早く返事しており、情報の価値によると、お互いに価格を合意します。

取引方式

ビットコインで取引するのをお勧めです。

連絡方法

メール：[redacted]
我々はなるべく迅速に君とコンタクトします。ＰＧＰによる暗号化通信を推薦して、右側には僕のＧＰＧ公開鍵です。よろしくお願いします。

PGP key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
[redacted]
```

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

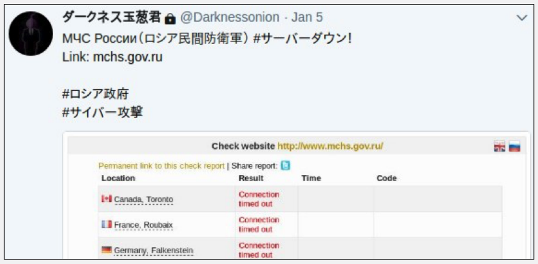
Hacktivism is particularly prevalent in Japan. Japanese hacktivists are mostly concerned with environmental issues, but overall can be divided into four categories:

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.



ダークネス玉葱君 @Darknessonion · Jan 5

МЧС России（ロシア民間防衛軍）#サーバーダウン!
Link: mchs.gov.ru

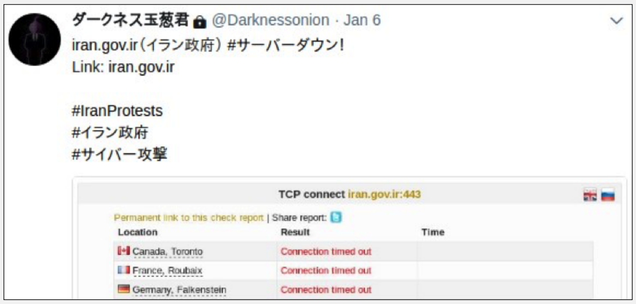
#ロシア政府
#サイバー攻撃

Check website http://www.mchs.gov.ru/

Permanent link to this check report | Share report:

Location	Result	Time	Code
Canada, Toronto	Connection timed out		
France, Roubaix	Connection timed out		
Germany, Falkenstein	Connection timed out		

Image 8: invitation from Japanese threat actor to take a part in a Japanese hacking group.



ダークネス玉葱君 @Darknessonion · Jan 6

iran.gov.ir（イラン政府）#サーバーダウン!
Link: iran.gov.ir

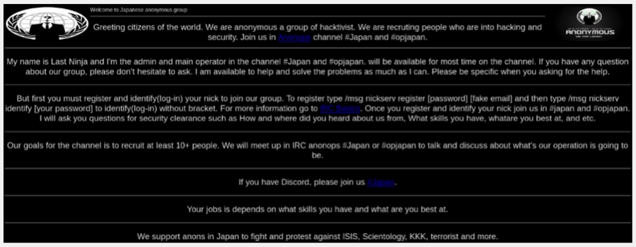
#IranProtests
#イラン政府
#サイバー攻撃

TCP connect iran.gov.ir:443

Permanent link to this check report | Share report:

Location	Result	Time
Canada, Toronto	Connection timed out	
France, Roubaix	Connection timed out	
Germany, Falkenstein	Connection timed out	

Image 9: An attack carried out by Darkness Onion-kun on the Iranian Portal for Government Services.



Welcome to Japanese anonymous group

Greeting citizens of the world. We are anonymous a group of hacktivist. We are recruting people who are into hacking and security. Join us in Anonops channel #Japan and #opjapan.

My name is Last Ninja and I'm the admin and main operator in the channel #Japan and #opjapan. will be available for most time on the channel. If you have any question about our group, please don't hesitate to ask. I am available to help and solve the problems as much as I can. Please be specific when you asking for the help.

But first you must register and identify(log-in) your nick to join our group. To register type /msg nickserv register [password] [fake email] and then type /msg nickserv identify [your password] to identify(log-in) without bracket. For more information go to IRC Basics. Once you register and identify your nick join us in #japan and #opjapan. I will ask you questions for security clearance such as How and where did you heard about us from, What skills you have, whatare you best at, and etc.

Our goals for the channel is to recruit at least 10+ people. We will meet up in IRC anonops #Japan or #opjapan to talk and discuss about what's our operation is going to be.

If you have Discord, please join us #Japan.

Your jobs is depends on what skills you have and what are you best at.

We support anons in Japan to fight and protest against ISIS, Scientology, KKK, terrorist and more.

Image 10: Anonymous Japan splash page

JAPAN'S THREAT ACTORS

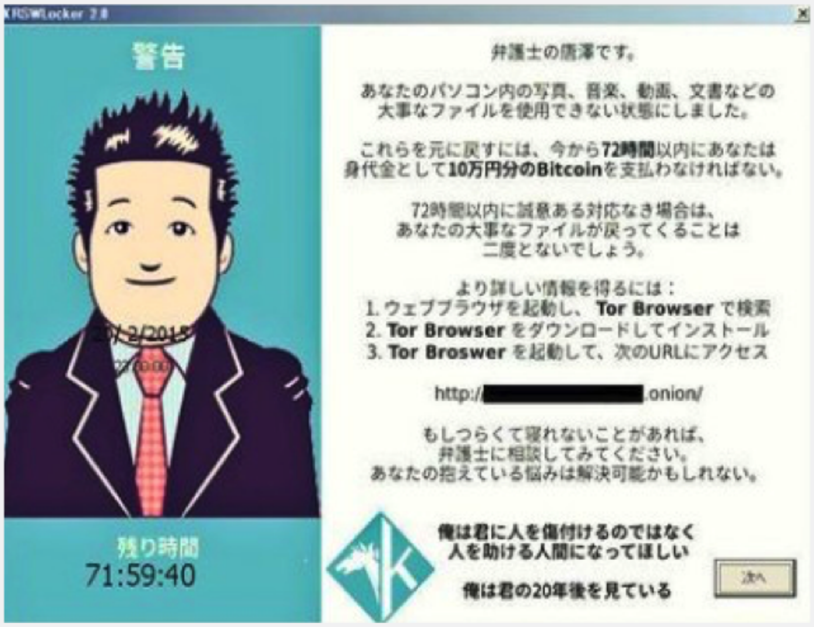
0chiaki

Born in 1997, 0chiaki is the writer of Japan's first ransomware: ***Karansomware***[1]. 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 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.



弁護士の唐澤です。

あなたのパソコン内の写真、音楽、動画、文書などの
大事なファイルを使用できない状態にしました。

これらを元に戻すには、今から**72時間**以内にあなたは
身代金として**10万円分のBitcoin**を支払わなければない。

72時間以内に誠意ある対応なき場合は、
あなたの大事なファイルが戻ってくることは
二度とないでしょう。

より詳しい情報を得るには：
1. ウェブブラウザを起動し、**Tor Browser** で検索
2. **Tor Browser** をダウンロードしてインストール
3. **Tor Broswer** を起動して、次のURLにアクセス

http:/[redacted].onion/

もしつらくて寝れないことがあれば、
弁護士に相談してみてください。
あなたの抱えている悩みは解決可能かもしれない。

俺は君に人を傷付けるのではなく
人を助ける人間になってほしい

俺は君の20年後を見ている

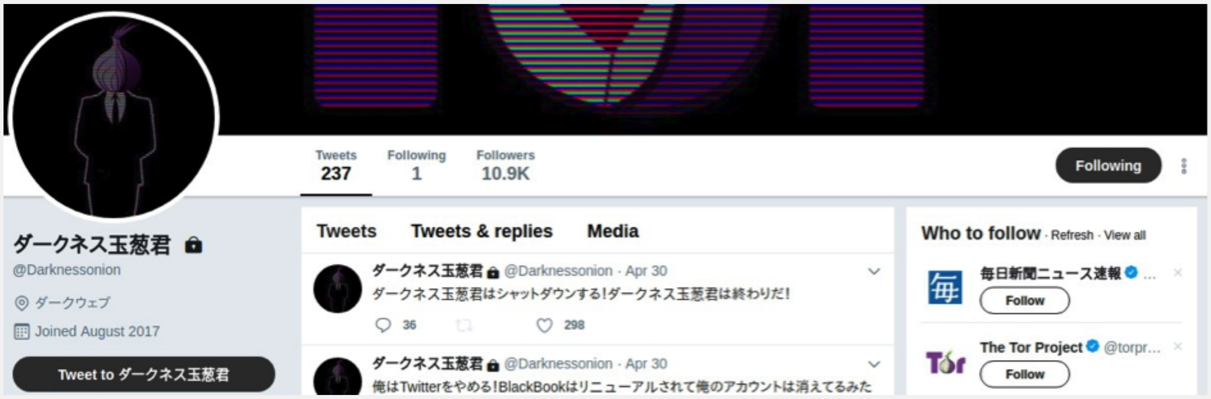
Image 11: Karansomware's lock screen

Darkness Onion-kun[2]

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.



ダークネス玉葱君
@Darknessonion
ダークウェブ
Joined August 2017

Tweets 237 | Following 1 | Followers 10.9K

ダークネス玉葱君 @Darknessonion · Apr 30
ダークネス玉葱君はシャットダウンする!ダークネス玉葱君は終わりだ!
36 298

ダークネス玉葱君 @Darknessonion · Apr 30
俺はTwitterをやめる!BlackBookはリニューアルされて俺のアカウントは消えてるみた

Who to follow · Refresh · View all
毎日新聞ニュース速報 ...
The Tor Project @torpr...

Image 12: Darkness Onion-kun Twitter Page

CHINA

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 Bar***[3] (Baidu Tieba), which is a communication platform as part of the Baidu search engine. Another platform is ***Baidu Knows***[4] (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***[16]), 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***[17], 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.

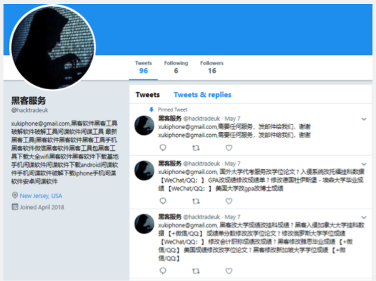
Drugs / Narcotics: Many Chinese drug vendors began to understand that operating using the Chinese web might be too risky. Therefore, around 2014 they started to move into dark web black markets. Some use Chinese websites like Mushroom, which offers many types and different brands of drugs. Others are 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 Xueli***[5]***"***, 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.



黑客服务
@hacktradeuk

xukiphone@gmail.com,黑客软件黑客工具破解软件破解工具间谍软件间谍工具 最新黑客工具|黑客软件黑客软件黑客工具手机黑客软件微信黑客软件黑客工具包黑客工具下载大全wifi黑客软件黑客软件下载基地手机间谍软件间谍软件下载android间谍软件手机间谍软件破解下载iphone手机间谍软件安卓间谍软件

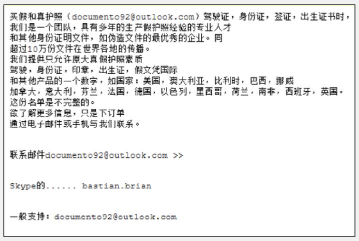
New Jersey, USA
Joined April 2018

黑客服务 @hacktradeuk · May 7
xukiphone@gmail.com,需要任何服务，发邮件给我们，谢谢
xukiphone@gmail.com,需要任何服务，发邮件给我们，谢谢

黑客服务 @hacktradeuk · May 7
xukiphone@gmail.com, 国外大学代考服务改学位论文？入侵系统改托福挂科数据【WeChat/QQ: 】GPA改成绩修改成绩单？修改德国杜伊斯堡 - 埃森大学毕业成绩【WeChat/QQ: 】美国大学改gpa改博士成绩

黑客服务 @hacktradeuk · May 7
xukiphone@gmail.com, 黑客改大学成绩改挂科成绩？黑客入侵加拿大大学挂科数据【+微信/QQ:】成绩单分数修改改学位论文？修改俄罗斯大学学位成绩【WeChat/QQ: 】修改会计职称成绩改成绩？黑客修改雅思毕业成绩【+微信/QQ:】美国成绩修改改学位论文？黑客修改新加坡大学学位成绩【+微信/QQ:】

Image 13: Example of changing GPA and hacking services



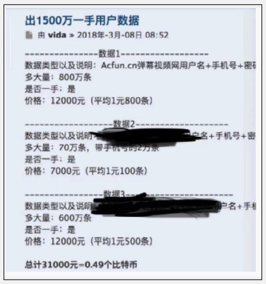
买假和真护照（documento92@outlook.com）驾驶证，身份证，签证，出生证书时，
我们是一个团队，具有多年的生产假护照经验的专业人才
和其他身份证明文件，如伪造文件的最优秀的企业。同
超过10万份文件在世界各地的传播。
我们提供只允许原大真假护照素质
驾驶，身份证，印章，出生证，假文凭国际
和其他产品的一个数字，如国家：美国，澳大利亚，比利时，巴西，挪威
加拿大，意大利，芬兰，法国，德国，以色列，墨西哥，荷兰，南非，西班牙，英国。
这份名单是不完整的。
欲了解更多信息，只是下订单
通过电子邮件或手机与我们联系。

联系邮件documento92@outlook.com >>

Skype的...... bastian.brian

一般支持：documento92@outlook.com

Image 14: Fake and real passports, I.D cards and driver's licenses for sale



出1500万一手用户数据
由 vida » 2018年-3月-08日 08:52

---------------数据1------------------
数据类型以及说明：Acfun.cn弹幕视频网用户名+手机号+密码
多大量：800万条
是否一手：是
价格：12000元（平均1元800条）

------------------数据2-------------------
数据类型以及说明[redacted]户名+手机号+密
多大量：70万条，带手机号的2万条
是否一手：是
价格：7000元（平均1元100条）

----------------数据3-[redacted]
数据类型以及说明[redacted]户名+手机
多大量：600万条
是否一手：是
价格：12000元（平均1元500条）

总计31000元=0.49个比特币

Image 15: AcFun's 15 million user records for sale on a dark web forum

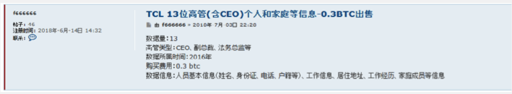
Bank Account and Credit Card Information: Just like any black market, financial information is a popular "good" across Chinese black markets. Credit card and bank account information are called "Material" in Chinese (***Liao***[7]). "Material washing men" (***Xi Liao Ren***[8]) are the people that sell information on the underground markets. Material master (***Liao Zhu***[9]) are the criminals who steal and sell bank account information. Envelope (***Xin Feng***[10]) 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***[11]", 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[12]" (***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***[13], ***Chezhu***[14], ***Daxia***[15]) 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.

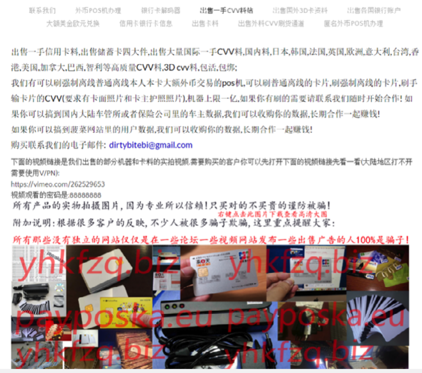


f666666
帖子：46
注册时间：2018年-6月-14日 14:32
联系：

TCL 13位高管(含CEO)个人和家庭等信息-0.3BTC出售
由 f666666 » 2018年-7月-03日 22:20

数据量：13
高管类型：CEO、副总裁、法务总监等
数据所属时间：2016年
购买费用：0.3 btc
数据信息：人员基本信息(姓名、身份证、电话、户籍等)、工作信息、居住地址、工作经历、家庭成员等信息

Image 16: Personal and family information of 13 TCL executives for sale



出售一手信用卡料,出售储蓄卡四大件,出售大量国际一手CVV料,国内料,日本,韩国,法国,英国,欧洲,意大利,台湾,香港,美国,加拿大,巴西,智利等高质量CVV料,3D cvv料,包活,包绑;

我们有可以刷强制离线普通离线本人本卡大额外币交易的pos机,可以刷普通离线的卡片,刷强制离线的卡片,刷手输卡片的CVV(要求有卡面照片和卡主护照照片),机器上限一亿,如果你有刷的需要请联系我们随时开始合作! 如果你可以搞到国内大陆车管所或者保险公司里的车主数据,我们可以收购你的数据,长期合作一起赚钱!

如果你可以搞到菠菜网站里的用户数据,我们可以收购你的数据,长期合作一起赚钱!

购买联系我们的电子邮件: dirtybitebi@gmail.com

下面的视频链接是我们出售的部分机器和卡料的实拍视频,需要购买的客户你可以先打开下面的视频链接先看一看(大陆地区打不开需要使用V/PN):
https://vimeo.com/262529653
视频观看的密码是:88888888

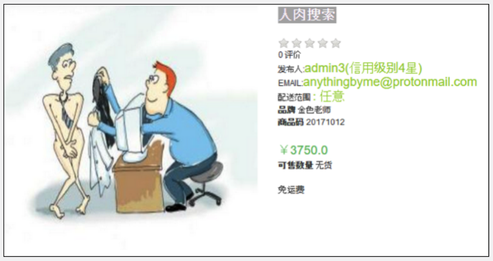
所有产品的实物拍摄图片，因为专业所以信赖!只买对的不买贵的谨防被骗!

右键点击此图片下载查看高清大图

附加说明：根据很多客户的反映，不少人被很多骗子欺骗，这里重点提醒大家：

所有那些没有独立的网站仅仅是在一些论坛一些视频网站发布一些出售广告的人100%是骗子!

Image 17: CVV (credit card information) for sale



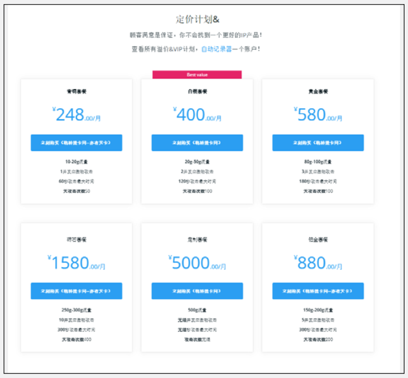
人肉搜索

☆☆☆☆☆
0 评价
发布人:admin3(信用级别4星)
EMAIL:anythingbyme@protonmail.com
配送范围：任意
品牌 金色老师
商品码 20171012

￥3750.0
可售数量 无货

免运费

Image 18: Post for doxing services



定价计划&
顾客满意是保证，你不会找到一个更好的IP产品!
查看所有溢价&VIP计划，自动记录器一个账户!

Best value

青铜套餐	白银套餐	黄金套餐
¥248.00/月	¥400.00/月	¥580.00/月
[illegible]	[illegible]	[illegible]
10-20g流量	20g-50g流量	80g-100g流量
1并发攻击数攻击	2并发攻击数攻击	3并发攻击数攻击
60秒攻击最大时间	120秒攻击最大时间	180秒攻击最大时间
天攻击次数50	天攻击次数100	天攻击次数100

钻石套餐	定制套餐	铂金套餐
¥1580.00/月	¥5000.00/月	¥880.00/月
[illegible]	[illegible]	[illegible]
250g-300g流量	500g流量	150g-200g流量
10并发攻击数攻击	无限并发攻击数攻击	5并发攻击数攻击
300秒攻击最大时间	无限秒攻击最大时间	300秒攻击最大时间
天攻击次数400	攻击次数无限	天攻击次数200

Image 19: DDoS prices and packaging

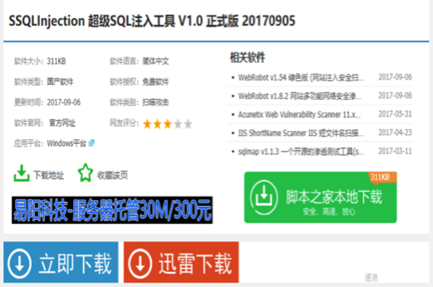
Hacking-as-a-Service: Individual hackers and hacking groups offer hacking services, including social media and bank account takeovers, DDoS, defacement, Doxing, website hacking, writing zero-day exploits, source code stealing, spam services, and phishing. All of these services can be customized to fit 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.

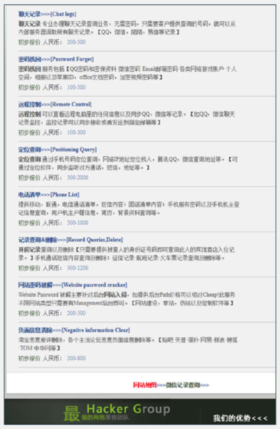
Human Organs Trade: During our research, we discovered posts in a few dark web forums and telegram channels from people who offered human organs for sale.


SSQLInjection 超级SQL注入工具 V1.0 正式版 20170905

软件大小：311KB　软件语言：简体中文
软件类型：国产软件　软件授权：免费软件
更新时间：2017-09-06　软件类别：扫描攻击
软件官网：官方网址　网友评分：★★★☆☆
应用平台：Windows平台

相关软件
- WebRobot v1.54 绿色版 (网站注入安全扫... 2017-09-06
- WebRobot v1.8.2 网站多功能网络安全渗... 2017-09-06
- Acunetix Web Vulnerability Scanner 11.x... 2017-05-31
- IIS ShortName Scanner IIS 短文件名扫描... 2017-04-23
- sqlmap v1.1.3 一个开源的渗透测试工具(s... 2017-03-11

Image 20: SQL Injection


聊天记录>>>[Chat logs]
聊天记录 专业办理聊天记录查询业务，无需密码，只需要客户提供查询的号码，就可以从内部服务器调取所有聊天记录。【QQ，微信，陌陌，易信等记录】
初步报价 人民币： 200-500

密码找回>>>[Password Forget]
密码找回 服务包括【QQ密码和密保资料 微信密码 Email邮箱密码 各类网络游戏账户 个人空间，相册以及苹果ID，office文档密码，加密视频密码等】
初步报价 人民币： 100-500

远程控制>>>[Remote Control]
远程控制 可以查看远程电脑里的任何信息以及同步QQ，微信等记录。【如QQ，微信聊天记录监控，监控记录可以同步接收或者发送到指定邮箱等】
初步报价 人民币： 100-300

定位查询>>>[Positioning Query]
定位查询 通过手机号码定位查询，网络IP地址定位找人，腾讯QQ，微信查询地址等。【可通过定位软件，同步监听对方通话，短信，地址等。】
初步报价 人民币： 300-2000

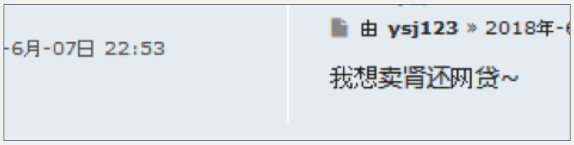
电话清单>>>[Phone List]
提供移动，联通，电信通话清单，短信内容；固话清单内容；手机服务密码以及手机机主登记信息查询，用户机主户籍信息，简历，背景资料查询等。
初步报价 人民币： 200-1000

记录查询&删除>>>[Record Queries,Delete]
开房记录查询以及删除【只需要提供被查人的身份证号码即可查询此人的宾馆酒店入住记录。】手机通话短信内容查询及删除；征信记录·航班记录·火车票记录查询及删除等。
初步报价 人民币： 300-1200

网站密码破解>>>[Website password cracker]
Website Password 破解主要针对后台网站入侵，如提供后台Path价格可以相对Cheap!此服务不限网站类型只需要有Management后台即可。【网站建设，拿站，仿站以及定制软件等】
初步报价 人民币： 200-500

负面信息清除>>>[Negative information Clear]
淘宝恶意差评删除，各个主流论坛恶意负面信息删除等。【贴吧·天涯·猫扑·网易·新浪·搜狐·TOM·中华网等】
初步报价 人民币： 200-800

Image 21: Hacking services pricing list


-6月-07日 22:53

由 ysj123 » 2018年-(

我想卖肾还网贷~

Image 22: 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.

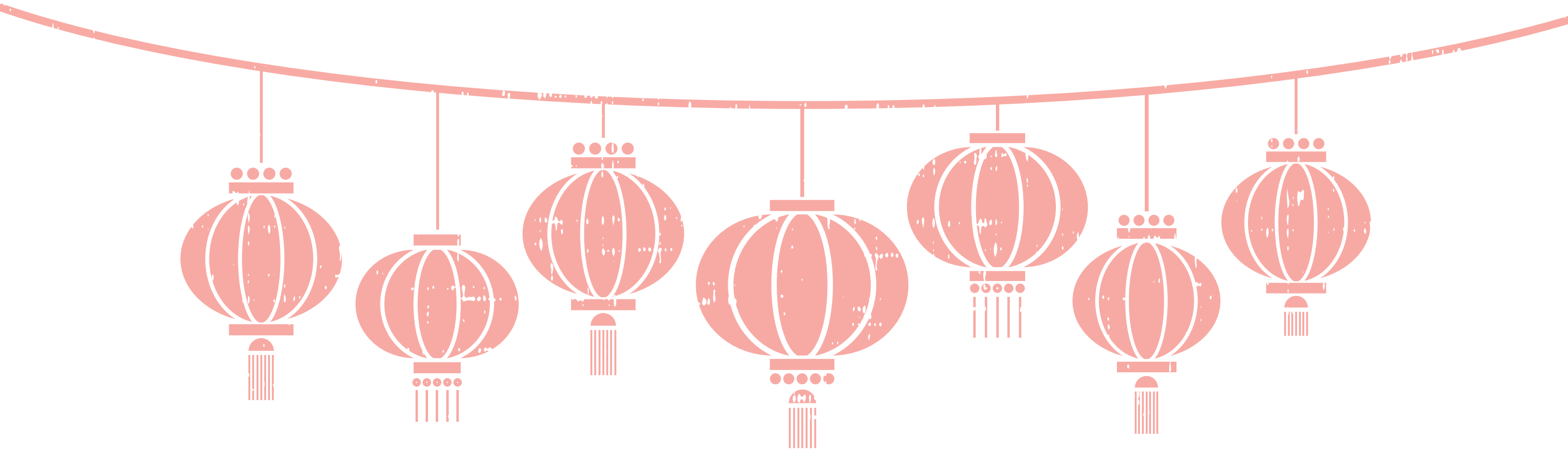
Stealing Foreign Intellectual Property: This is done for the sake of advancing Chinese interests and is sometimes being conducted by state-affiliated hacking groups.

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. ***Fangongheike***[23] 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 Hacker***[24]" (Hongke, which literally means "red visitor"), as compared to the usual Chinese transliteration of hacker (***hēikè***[25], which literally means "Black Guest", as in black hat). The riots have also led to the formation of the Red Hacker Alliance (***Zhongguo Hongke Lianmeng***[26]). 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".

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.

Image 23: Goodwell (Gong Wei)

Goodwell: His real name is ***Gong Wei***[18]. 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.

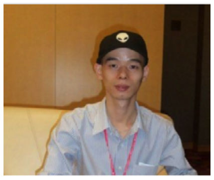


Image 24: Lion (Lin Yong)

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.

Image 25: Wan Tao (Eagle)

Wan Tao[19]**:** His nickname was ***Eagle***[20]. 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.

Image 26: Glacier (Huang Xin)

Glacier[21]**:** His real name is ***Huang Xin***[22]. 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.

January 21, 2013

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.

January 28, 2013

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.

March 28, 2015

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.

June 2016

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 "***programthink***[27]", 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.

February 28, 2018

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.

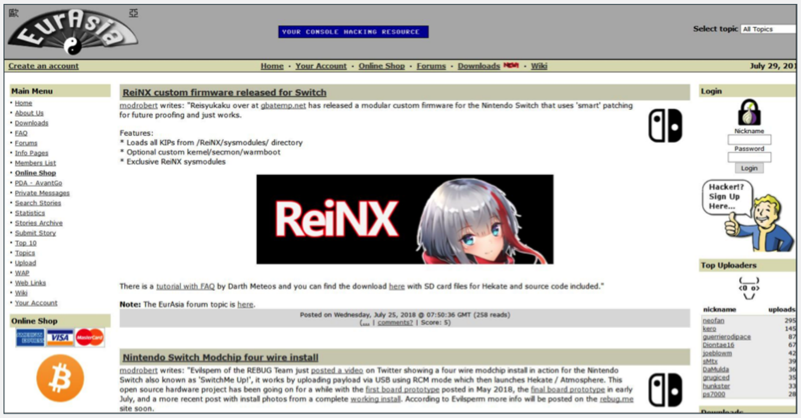
Most of the South Korean dark web sites are used for illegal activity. These sites are relatively small compared to the number of Internet users in the country, but activity has increased over the past few years.

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.



ReiNX custom firmware released for Switch

modrobert writes: "Reisyukaku over at gbatemp.net has released a modular custom firmware for the Nintendo Switch that uses 'smart' patching for future proofing and just works.

Features:
* Loads all KIPs from /ReiNX/sysmodules/ directory
* Optional custom kernel/secmon/warmboot
* Exclusive ReiNX sysmodules

There is a tutorial with FAQ by Darth Meteos and you can find the download here with SD card files for Hekate and source code included."

Note: The EurAsia forum topic is here.

Posted on Wednesday, July 25, 2018 @ 07:50:36 GMT (258 reads)
(... | comments? | Score: 5)

Nintendo Switch Modchip four wire install

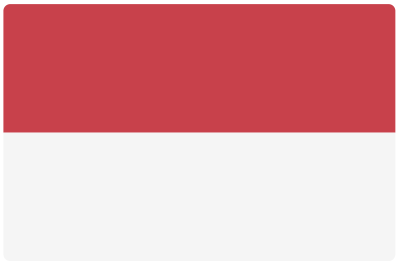
modrobert writes: "Evilspem of the REBUG Team just posted a video on Twitter showing a four wire modchip install in action for the Nintendo Switch also known as 'SwitchMe Up!', it works by uploading payload via USB using RCM mode which then launches Hekate / Atmosphere. This open source hardware project has been going on for a while with the first board prototype posted in May 2018, the final board prototype in early July, and a more recent post with install photos from a complete working install. According to Evilsperm more info will be posted on the rebug.me site soon.

nickname	uploads
neofan	295
kero	145
guerrierodipace	87
Diontae16	67
joeblowm	42
sMtx	39
DaMulda	36
gruqiced	35
hunkster	33
ps7000	28

Image 27: Popular South Korean black market (EurAsia)

INDONESIA

A Dark Web for Black Markets and Blackjack



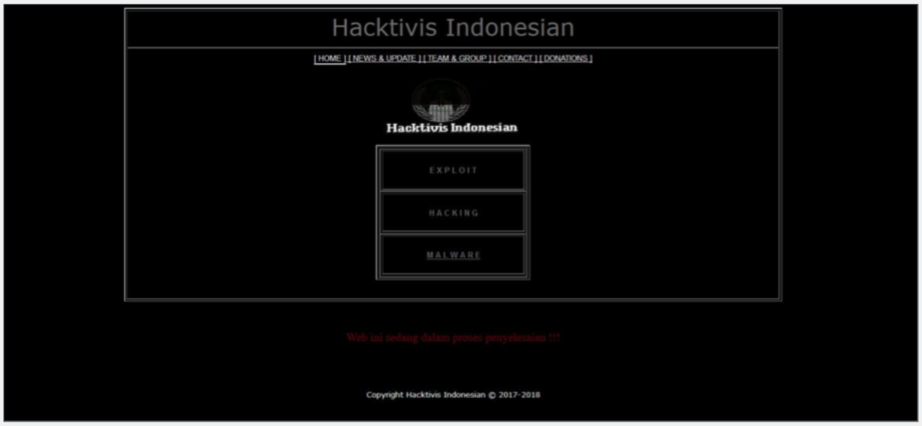
BACKGROUND

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



Hacktivis Indonesian

[HOME] [NEWS & UPDATE] [TEAM & GROUP] [CONTACT] [DONATIONS]
Hacktivis Indonesian
EXPLOIT
HACKING
MALWARE

Web ini sedang dalam proses penyelesaian !!!

Copyright Hacktivis Indonesian © 2017-2018

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 ground-breaking 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.

INTSIGHTS

Threat Intelligence Realized.