The Japanese Underground

Akira Urano
Forward-Looking Threat Research (FTR) Team

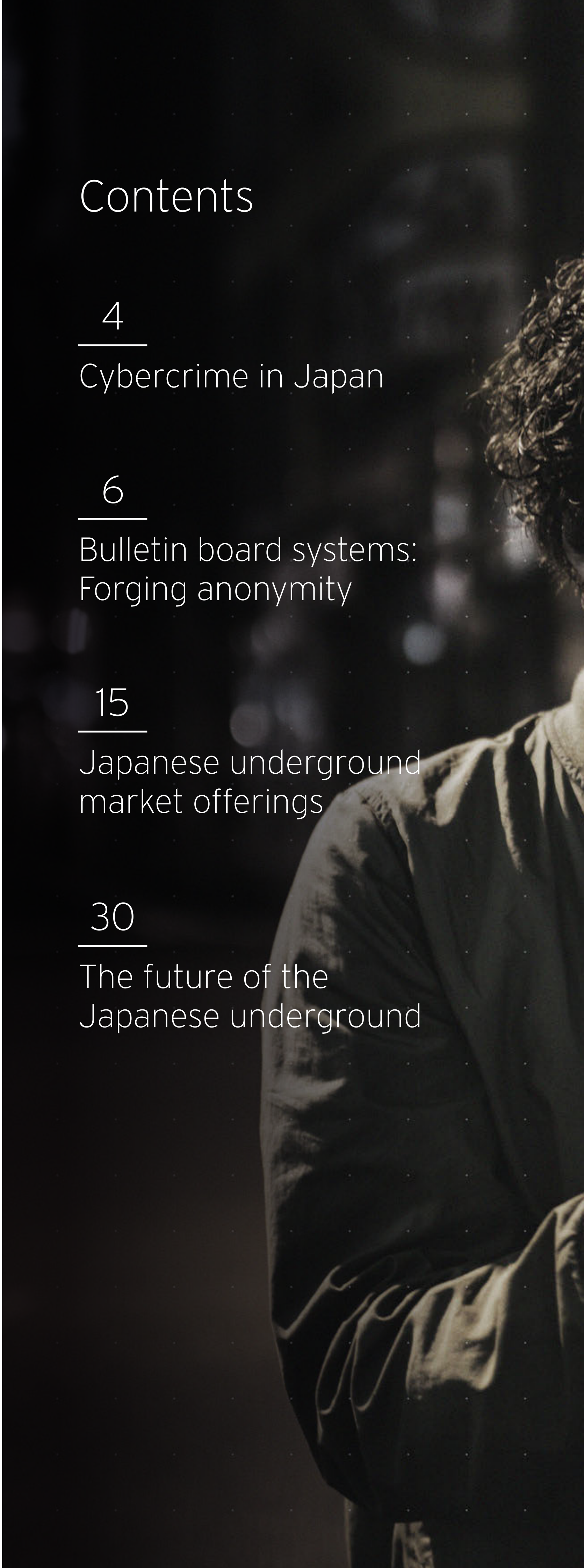
A **TrendLabs**SM Research Paper

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



Contents

Japan is a country of balanced contrasts. It is well-known not only for its homegrown automated advancements, but also for its conservative outlook in adopting outside technologies. In terms of cybercrime, its own underground economy is still fairly younger and smaller compared with its foreign counterparts. The country's strict legislation against crime has influenced an underground that veers away from malware creation and transforms into its own entity—a marketplace characterized by the taboo, the illegal, and the vindictive.

Instead of creating their own attack tools from scratch, Japanese cybercriminals instead purchase what they need from foreign peers at competitive prices. Offerings in the Japanese underground are often found on gated bulletin boards that screen users, creating a distinct, localized environment. On these forums, anonymous users can discuss prohibited topics or buy and sell illegal products and services.

The exclusivity and anonymity that the Japanese underground offers may become attractive to organized criminal groups in the future. This inevitably puts pressure on law enforcement agencies like the National Police Agency (NPA) to set up countermeasures against cybercrime in the country.

This underground economy paper, the first for Japan, offers a glimpse into a unique cybercriminal economy. It complements our research on the thriving cybercriminal marketplaces in Russia[1], Brazil[2], and China[3].

SECTION 1

Cybercrime in Japan

Cybercrime in Japan

A report by the Japan NPA shows that queries about potential online crime cases have gone up nearly 40% in March 2015 from the previous year. For a country that has a relatively high Internet penetration rate of 86% off a base population of nearly 127 million[4], a 40% increase is a big deal. The financial damage from illegal online bank transfers in 2014 amounted to roughly ¥2.91 billion or US$24 million[5] while the total estimated online fraud damage cost banks ¥1.54 billion or US$13 million in the first half of 2015[6]*. The NPA also revealed that financial losses could be attributed to online fraudsters who used stolen IDs and passwords.

Data from the Trend Micro™ Smart Protection Network™ showed that Japan was the second most affected country by online banking malware in 2014, following the United States[7]. As of the second quarter of this year, the country was also most affected by Angler-Exploit-Kit-related activity (49%)[8].

A June cyber attack on the Japan Pension Service was among the high-profile cases seen this second quarter where more than a million victims' personal data was exposed[9]. The data leaked included employees' names, ID numbers, dates of birth, and even home addresses.

Despite the above-mentioned numbers on previously targeted entities, the Japanese cybercriminal underground is still in its infancy. Japanese cybercriminals are still learning how to use various tools of the trade. They continuously acquire knowledge on malware creation via online hacker forums.

** Currency exchange rate as of 29 September 2015 was used for all conversions in this paper (US$1 = ¥119.74).*

SECTION 2

Bulletin board systems: Forging anonymity

Bulletin board systems: Forging anonymity

Bulletin board systems (BBSs) play a big role in helping the Japanese cybercriminal underground economy thrive. A BBS is a computer or an application dedicated to the sharing or exchange of messages or other files on a network[10]. Once logged in via a terminal program, users can exchange messages via chat, email, and public message boards.

A sense of community on BBSs was widely embraced in Japan with the introduction of the popular forum, 2channel, in 1999. Its BBS setup does not differ from the usual configurations seen in the United States (US). Its success in Japan influenced its US counterpart, 4chan, which offers the same services. 2channel is best known for the anonymity that it offers to its large user base. It grants users an outlet for unrestrained, free expression, without worrying about being ostracized[11].

Unfortunately, the anonymity that 2channel offers also makes it a suitable place for facilitating and committing cybercrime. It was notably abused in 2012 when Yusuke Katayama, a hacker better known as the “Demon Killer” spread malware in the forum to infiltrate and gain control of users’ computers[12]. Katayama was also eventually arrested in February 2013[13].

BBSs are mainly self-contained communities that offer users a little bit of everything via various message board forums. These forums can be used for anonymous discussions. They can also foster the buying and selling of illegal products and services or serve as repositories for hacking advice.

Japanese BBS features

Japanese BBSs exhibit a few unique characteristics that set them apart from underground forums found in other regions.

Entry points

Users can land on underground BBSs via several ways. They can ask around in forums or visit more popular and publicly accessible BBSs that contain URLs that point to underground locations. Some of these URLs can even be found in print. In Japan, certain books and magazines on the Deep Web contain site URLs, along with instructions to access them.

Secret jargon

Individuals on BBSs often use a secret language or jargon when selling illegal goods and services. This can be a means to mask illegal transactions. Only those who are interested in availing of illicit offerings would know what words to look for.

Payment methods

Japanese underground market players also prefer rather unconventional modes of payment like gift cards instead of cash. They are known to accept Amazon™ gift cards and PlayStation® Store codes. This may imply that unlike their foreign counterparts, Japanese cybercriminals prefer traditional bartering of goods rather than accepting bitcoins and WebMoney as payment.

CAPTCHA use

A lot of the underground BBSs we monitored used CAPTCHAs as a security measure. The CAPTCHA forms were usually in Japanese, which could mean the website owners were either native speakers of the language or wanted to ensure that only Japanese speakers could access their sites.

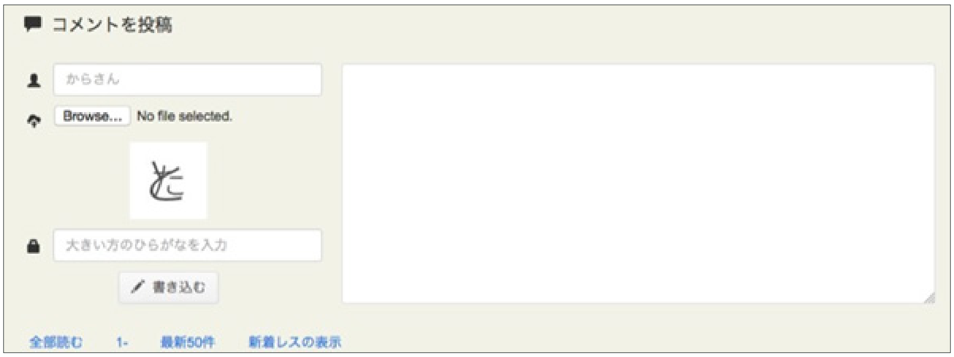
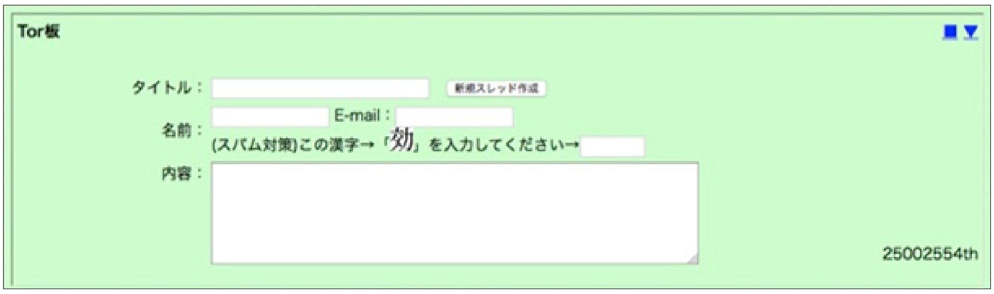


Figure 1: *CAPTCHA that asks visitors of “Koushinkyo,” a BBS, to enter the bigger Hiragana character (と) into the field in order to post a message*



Tor板

タイトル：

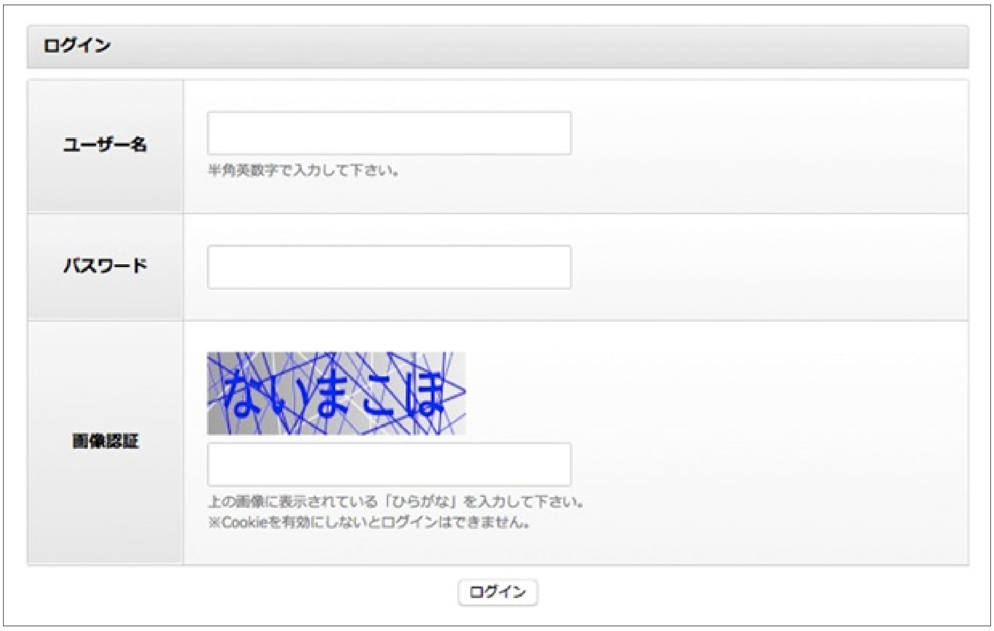
名前：　E-mail：

(スパム対策)この漢字→「効」を入力してください→

内容：

25002554th

Figure 2: *CAPTCHA that asks visitors of Tor 2 Channel to enter a Kanji character* (効) *to filter spam*



ログイン

ユーザー名

半角英数字で入力して下さい。

パスワード

画像認証

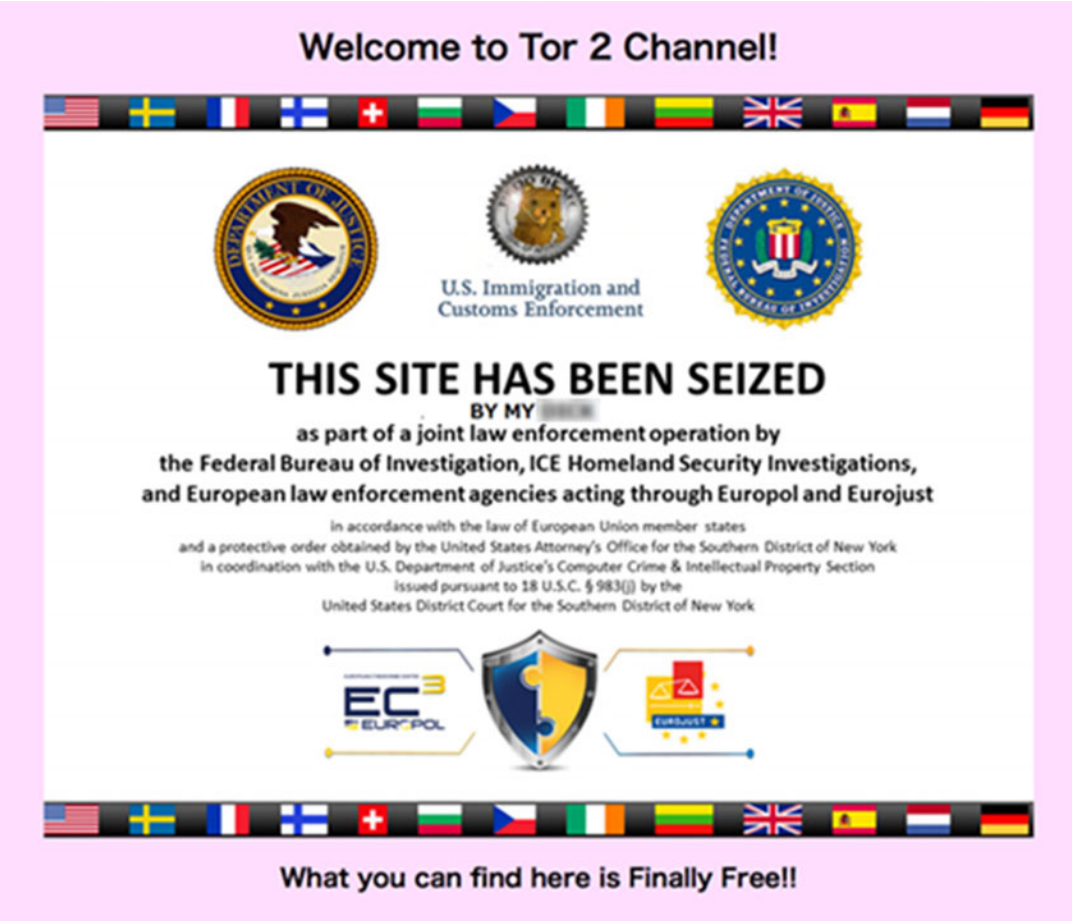
上の画像に表示されている「ひらがな」を入力して下さい。
※Cookieを有効にしないとログインはできません。

Figure 3: *CAPTCHA that asks visitors of Magical Onion, a child porn site,*
to enter Hiragana characters (ないまこほ) *in order to gain access*

Notable BBSs

The case of Tor 2 Channel

Constant monitoring of BBSs led us to a notable site named "The Onion Channel," also known as the "Tor 2 Channel." Accessing its URL displays a fake welcome page that contains several flags with embedded links pointing to the real site. Most of the topics discussed on Tor 2 Channel involve illegal and taboo dealings like mule services and drug trade. The forums found on Tor 2 Channel also give users access to a gold mine of products and services.



Welcome to Tor 2 Channel!

U.S. Immigration and Customs Enforcement

THIS SITE HAS BEEN SEIZED
BY MY [redacted]
as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

What you can find here is Finally Free!!

Figure 4: *Fake welcome page with clickable flags that lead to the real Tor 2 Channel page*

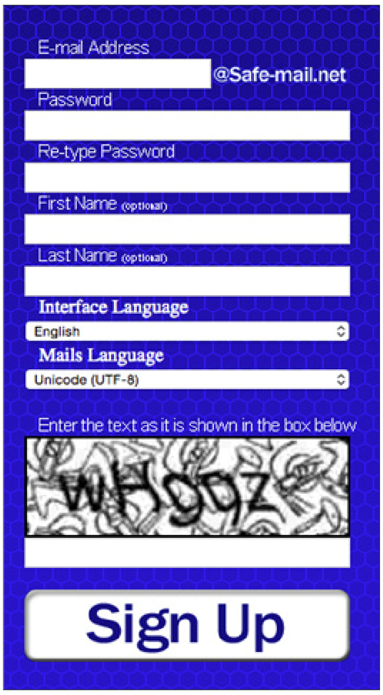
The URL we visited in order to access Tor 2 Channel had a .onion domain (*http://[REDACTED]72t7fd4jme.onion/*). Despite the warning that the site has been seized, hovering over the flags display several URLs that all lead to external sites (listed below) to access several BBSs.

- *http://[REDACTED]72t7fd4jmc.onion/toto/indexo.html*
- *http://[REDACTED]72t7fd4jmc.onion/toto/index.html*
- *http://[REDACTED]2kn32bo3ko.onion/ura/*
- *http://[REDACTED]2kn32bo3ko.onion/tor/*
- *http://[REDACTED]r66pehagee.onion/oops/ahan/*
- *http://[REDACTED]r66pehagee.onion/oops/tor2ch/*
- *http://[REDACTED]r66pehagee.onion/oops/tor2ch/*
- *http://[REDACTED]r66pehagee.onion/oops/yabb/bbs/ramdam/*
- *http://[REDACTED]r66pehagee.onion/oops/b32a/awhg/*
- *http://[REDACTED]r66pehagee.onion/oops/lgates/index.php*

To trade illegal items, BBS users utilize a secure communication service called “SAFe-mail[14].” Dark Web users have also shifted to this service known for its “secure, feature-rich messaging systems[15].”

Users who wish to sign up do not need to give their names. As such, their real identities are not tied to their SAFe-mail addresses.

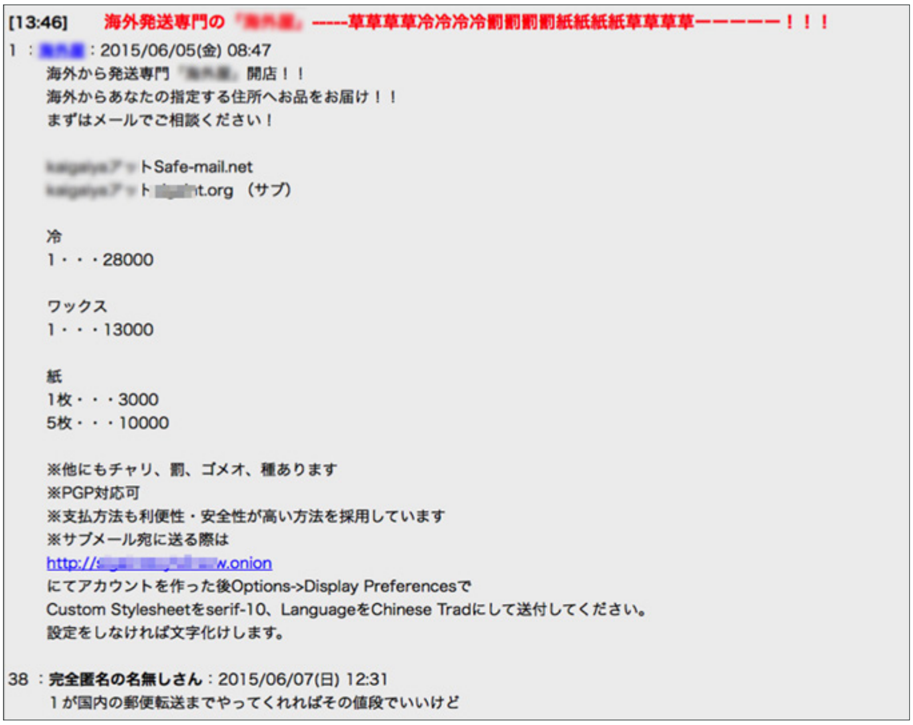
A Tor 2 Channel forum we monitored sold drugs but the wording used in posts did not mention any particular drug. Only a specific term was used to entice people willing to spend a few thousand yen on drugs. The site sold cannabis seeds to visitors who wish to grow their own plants and further their businesses.



Interface Language: English

Mails Language: Unicode (UTF-8)

Figure 5: *SAFe-mail’s sign-up form*



[13:46]　海外発送専門の「[redacted]」-----草草草草冷冷冷冷罰罰罰罰紙紙紙紙草草草草ーーーーーー！！！

1 ：[redacted]：2015/06/05(金) 08:47
海外から発送専門「[redacted]」開店！！
海外からあなたの指定する住所へお品をお届け！！
まずはメールでご相談ください！

[redacted]トSafe-mail.net
[redacted]ト[redacted]t.org （サブ）

冷
1・・・28000

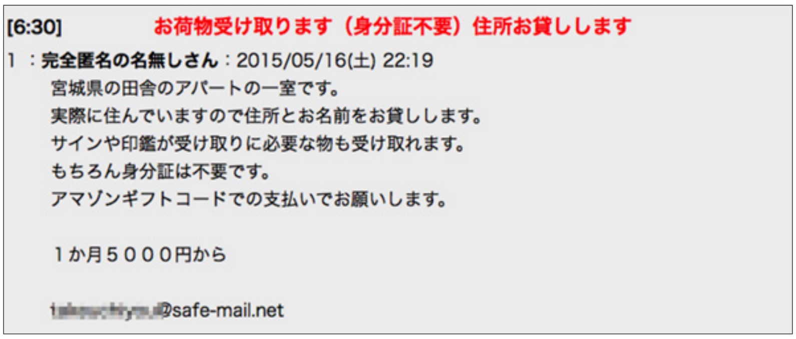
ワックス
1・・・13000

紙
1枚・・・3000
5枚・・・10000

※他にもチャリ、罰、ゴメオ、種あります
※PGP対応可
※支払方法も利便性・安全性が高い方法を採用しています
※サブメール宛に送る際は
http://[redacted]w.onion
にてアカウントを作った後Options->Display Preferencesで
Custom Stylesheetをserif-10、LanguageをChinese Tradにして送付してください。
設定をしなければ文字化けします。

38 ：**完全匿名の名無しさん**：2015/06/07(日) 12:31
１が国内の郵便転送までやってくれればその値段でいいけど

Figure 6: *Forum post in Tor 2 Channel with jargon pertaining to the sale of drugs ("cold or 冷," jargon for methamphetamine for ¥28,000 or US$234 per gram and "paper or ワックス," jargon for concentrated form of marijuana for ¥13,000 or US$109 per gram)*



[6:30]　お荷物受け取ります（身分証不要）住所お貸しします

1 ：**完全匿名の名無しさん**：2015/05/16(土) 22:19
宮城県の田舎のアパートの一室です。
実際に住んでいますので住所とお名前をお貸しします。
サインや印鑑が受け取りに必要な物も受け取れます。
もちろん身分証は不要です。
アマゾンギフトコードでの支払いでお願いします。

１か月５０００円から

[redacted]@safe-mail.net

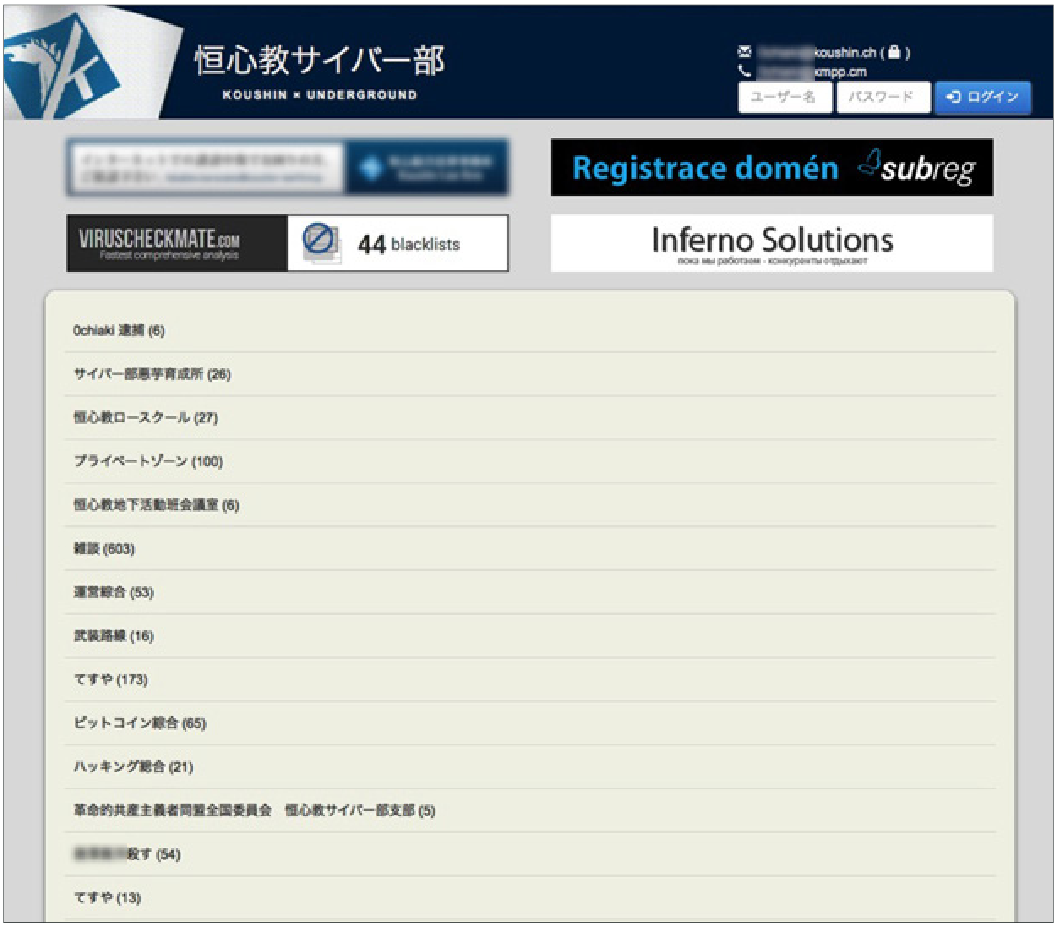
Figure 7: *Post in Tor 2 Channel that offers customers a receiving name (お名前) and address (住所) for their potentially illegal packages (money or goods) in exchange for a ¥5,000 or US$42 Amazon gift card code valid for a month (アマゾンギフトコードでの支払いでお願いします。)*

Tor 2 Channel also offers money mule services. Although this offering may be unusual in other markets, it seems to be a staple in the Japanese underground. What was notable in the post was that instead of money , the poster asked for an Amazon gift card code as payment.

The case of Ochiaki

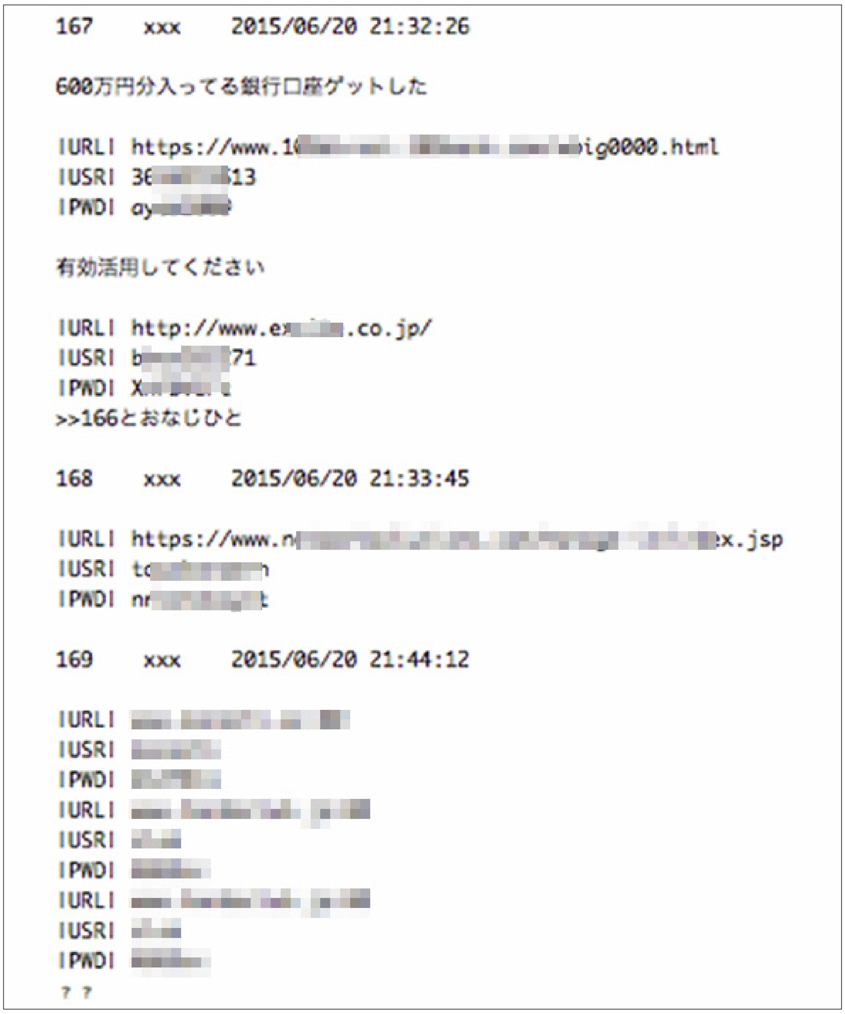
A BBS called "Koushin-kyo Cyber Division" (*http://[REDACTED]infmzibnzyd.onion/*), incidentally linked to the notorious hacker, 0chiaki, was also found. 0chiaki, a 17-year-old Japanese hacker, was arrested just this August for distributing ransomware[16], attempted hacking, and credit card fraud, among other crimes[17].

We looked at the BBS that 0chiaki previously managed and found that it currently does not have an owner. As of this writing, some threads on the BBS, including one called a "private zone," has been removed for unknown reasons. In some of these pages, we saw members share stolen account credentials and hacking information. Others discussed how to illegally make money. Koushin-kyo or "Koushin Underground" in English requires an invitation code from the owner before users can enter.



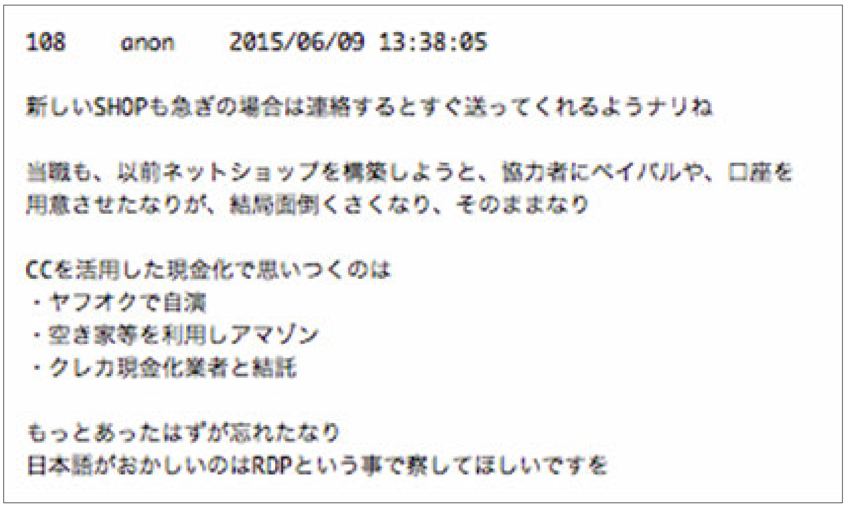
0chiaki 逮捕 (6)
サイバー部悪芋育成所 (26)
恒心教ロースクール (27)
プライベートゾーン (100)
恒心教地下活動班会議室 (6)
雑談 (603)
運営総合 (53)
武装路線 (16)
てすや (173)
ビットコイン総合 (65)
ハッキング総合 (21)
革命的共産主義者同盟全国委員会　恒心教サイバー部支部 (5)
[redacted]殺す (54)
てすや (13)

Figure 8: *Koushin Undergound's main page that shows links to pages containing details on 0chiaki's arrest (0chiaki 逮捕), cyberdivision training (サイバー部悪芋育成所), bitcoins (ビットコイン), a private zone (プライベートゾーン), and general hacking (ハッキング総合) and those that serve as meeting rooms for underground-related activities (恒心教地下活動班会議室)*



```
167    xxx    2015/06/20 21:32:26

600万円分入ってる銀行口座ゲットした

|URL| https://www.1[redacted]ig0000.html
|USR| 36[redacted]13
|PWD| ay[redacted]

有効活用してください

|URL| http://www.ex[redacted].co.jp/
|USR| b[redacted]71
|PWD| X[redacted]
>>166とおなじひと

168    xxx    2015/06/20 21:33:45

|URL| https://www.n[redacted]x.jsp
|USR| t[redacted]
|PWD| n[redacted]

169    xxx    2015/06/20 21:44:12

|URL| [redacted]
|USR| [redacted]
|PWD| [redacted]
|URL| [redacted]
|USR| [redacted]
|PWD| [redacted]
|URL| [redacted]
|USR| [redacted]
|PWD| [redacted]
? ?
```

Figure 9: *Sample Koushin Underground post that gives out credentials (usernames and passwords) for a bank account (銀行口座) containing ¥6 million or US$50,108*



```
108    anon    2015/06/09 13:38:05

新しいSHOPも急ぎの場合は連絡するとすぐ送ってくれるようナリね

当職も、以前ネットショップを構築しようと、協力者にペイパルや、口座を
用意させたなりが、結局面倒くさくなり、そのままなり

CCを活用した現金化で思いつくのは
・ヤフオクで自演
・空き家等を利用しアマゾン
・クレカ現金化業者と結託

もっとあったはずが忘れたなり
日本語がおかしいのはRDPという事で察してほしいですを
```

Figure 10: *Koushin Underground post that enumerates ways to get cash using credit cards (クレジットカード)—via Yahoo!® auctions (ヤフオク), having Amazon deliver to an uninhabited address (空き家), and working with traders who convert credit cards into actual money (CCを活用した現金化で思い付くのは)*

SECTION 3

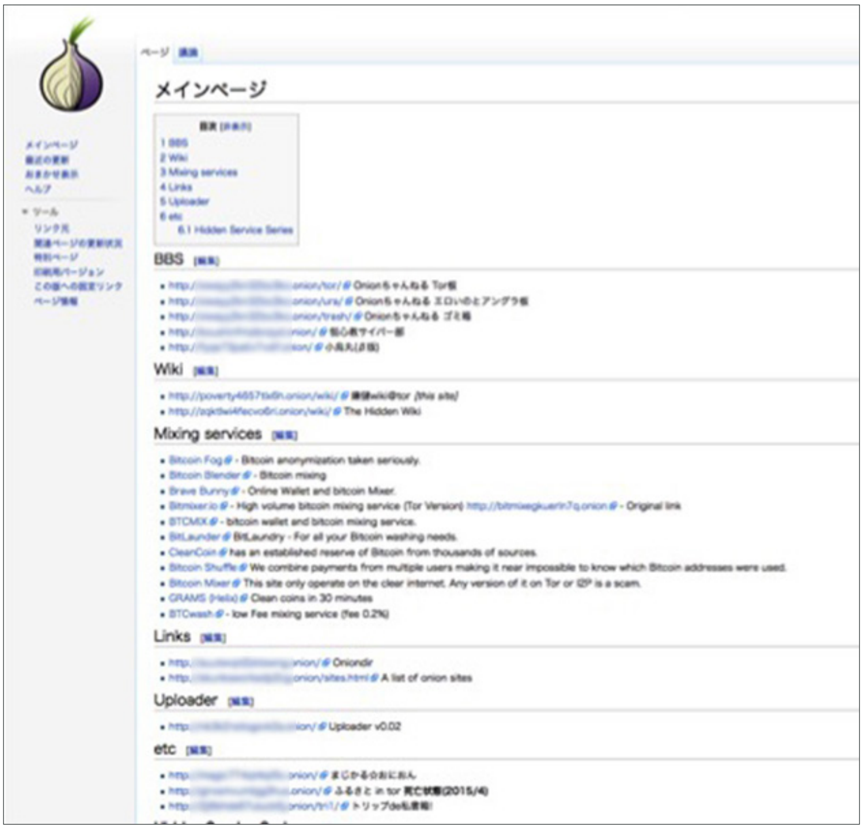
Japanese underground market offerings

Japanese underground market offerings

We used an internally developed system called “Deep Web Analyzer[18]” to closely observe the Deep Web. It collects URLs linked to the Deep Web, including The Onion Router (TOR)- and Invisible Internet Project (I2P)-hidden sites, Freenet resource identifiers, and domains with nonstandard top-level domains (TLDs) and tries to extract relevant information tied to these like page content, links, email addresses, HTTP headers, and so on.

For this particular research, we collected a total of 2,224 underground site URLs (all of which used Japanese) under 11 unique domains. Note that some of these sites were not related to cybercrime per se despite being hidden underground.

One such site, Ken-Mou wiki@Tor, contained a lot of links to bitcoin services and BBSs tied to other pages with illicit content. The related sites had information on child pornography, drugs, and other taboo subjects.



メインページ
最近の更新
おまかせ表示
ヘルプ

▼ ツール
リンク元
関連ページの更新状況
特別ページ
印刷用バージョン
この版への固定リンク
ページ情報

メインページ

目次 [非表示]
1 BBS
2 Wiki
3 Mixing services
4 Links
5 Uploader
6 etc
6.1 Hidden Service Series

BBS [編集]

- http://[redacted]onion/tor/ Onionちゃんねる Tor板
- http://[redacted]onion/ura/ Onionちゃんねる エロいのとアングラ板
- http://[redacted]onion/trash/ Onionちゃんねる ゴミ箱
- http://[redacted]onion/ 恒心教サイバー部
- http://[redacted]onion/ 小烏丸(β版)

Wiki [編集]

- http://poverty4657tx6h.onion/wiki/ 嫌儲wiki@tor *(this site)*
- http://sqkdwi4fecvo6ri.onion/wiki/ The Hidden Wiki

Mixing services [編集]

- Bitcoin Fog - Bitcoin anonymization taken seriously.
- Bitcoin Blender - Bitcoin mixing
- Brave Bunny - Online Wallet and bitcoin Mixer.
- Bitmixer.io - High volume bitcoin mixing service (Tor Version) http://bitmixegkuerln7q.onion - Original link
- BTCMIX - bitcoin wallet and bitcoin mixing service.
- BitLaunder BitLaundry - For all your Bitcoin washing needs.
- CleanCoin has an established reserve of Bitcoin from thousands of sources.
- Bitcoin Shuffle We combine payments from multiple users making it near impossible to know which Bitcoin addresses were used.
- Bitcoin Mixer This site only operate on the clear internet. Any version of it on Tor or I2P is a scam.
- GRAMS (Helix) Clean coins in 30 minutes
- BTCwash - low Fee mixing service (fee 0.2%)

Links [編集]

- http://[redacted]onion/ Oniondir
- http://[redacted]onion/sites.html A list of onion sites

Uploader [編集]

- http://[redacted]onion/ Uploader v0.02

etc [編集]

- http://[redacted]onion/ まじかる☆おにおん
- http://[redacted]onion/ ふるさと in tor 死亡状態(2015/4)
- http://[redacted]onion/tr1/ トリップde私書箱!

***Figure 11:** Ken-Mou wiki@Tor's wiki page, which contains URLs of BBSs, Web services, upload sites, and others*

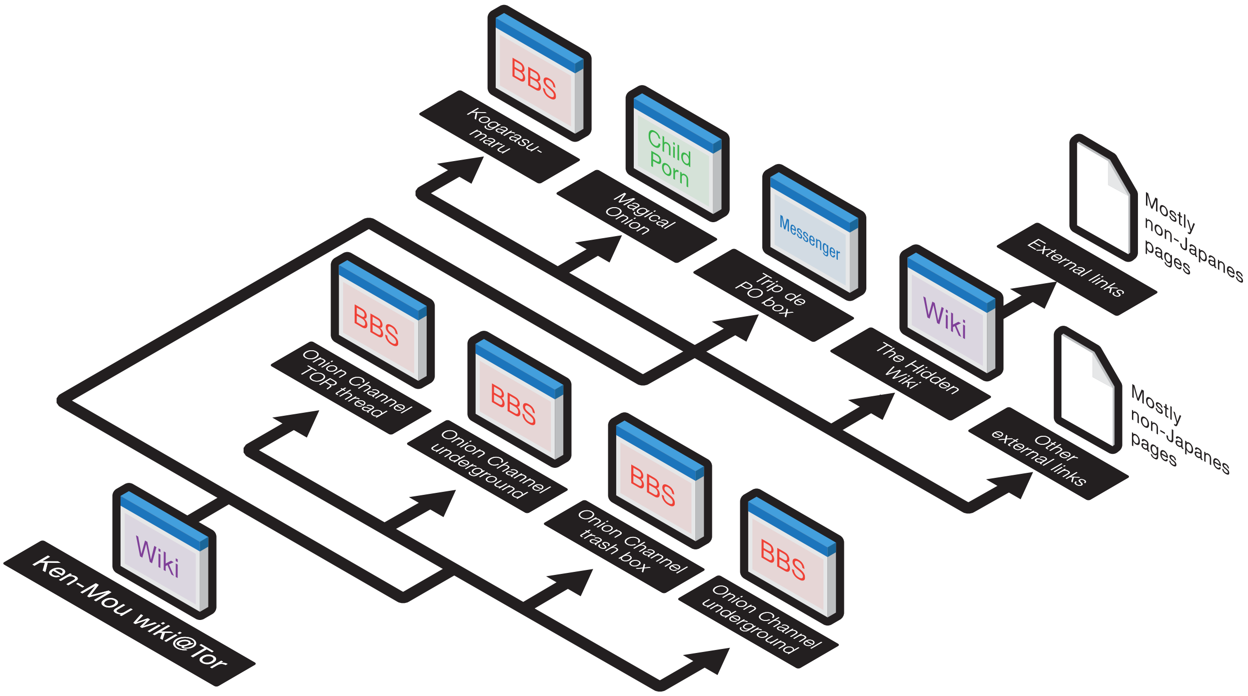
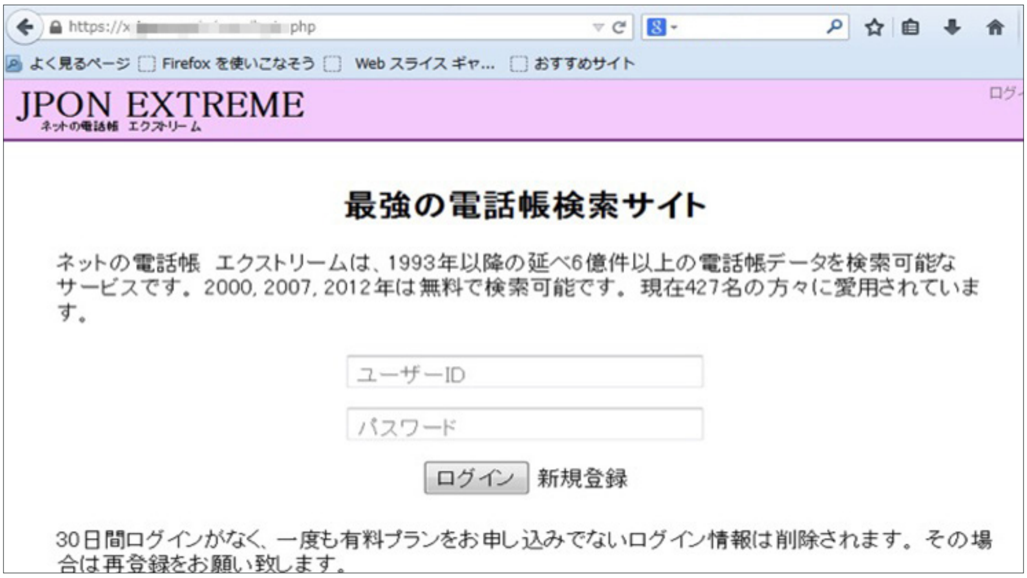


***Figure 12:** Ken-Mou wiki@Tor's site map*

Phone number databases

Phone number databases were among the offerings we found in the Japanese underground. These can be very useful to scammers. One of the sites called “JPON EXTREME” offers databases for download free of charge to all of its registered users. Where these databases came from remains unknown. It is unlikely though that they were legally retrieved from telecommunications companies.



JPON EXTREME
ネットの電話帳 エクストリーム

最強の電話帳検索サイト

ネットの電話帳 エクストリームは、1993年以降の延べ6億件以上の電話帳データを検索可能なサービスです。2000, 2007, 2012年は無料で検索可能です。現在427名の方々に愛用されています。

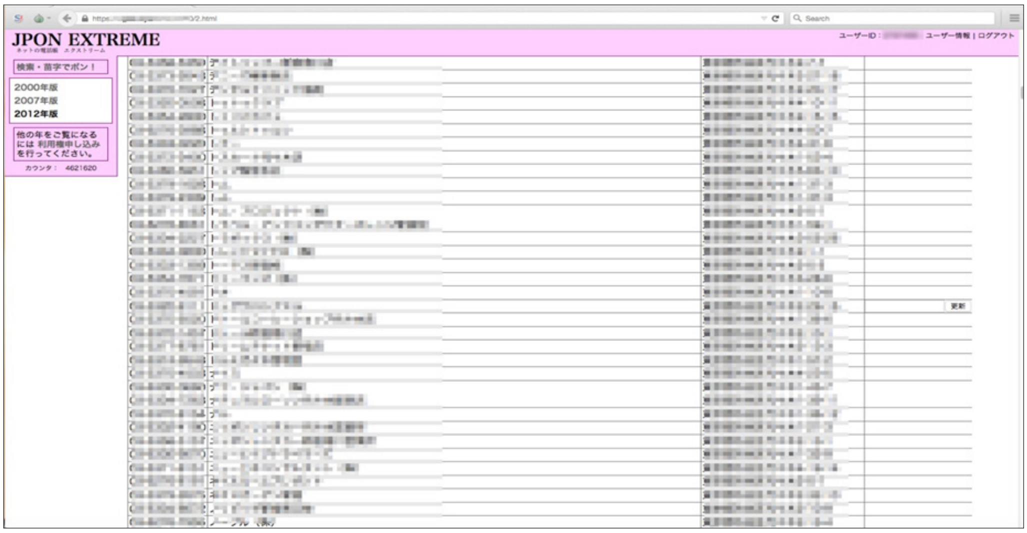
ユーザーID

パスワード

ログイン 新規登録

30日間ログインがなく、一度も有料プランをお申し込みでないログイン情報は削除されます。その場合は再登録をお願い致します。

Figure 13: *JPON EXTREME offers phone numbers collected in 2000, 2007, and 2012 to even unregistered users (Note that only registered users can get all other phone numbers stored in the database. The information also includes the owners’ names and addresses.)*


https://[redacted]/2.html
Search
JPON EXTREME
ネットの電話帳 エクストリーム
ユーザーID : [redacted] ユーザー情報 | ログアウト
検索・苗字でポン！
2000年版
2007年版
2012年版
他の年をご覧になるには 利用権申し込みを行ってください。
カウンタ： 4621620
更新

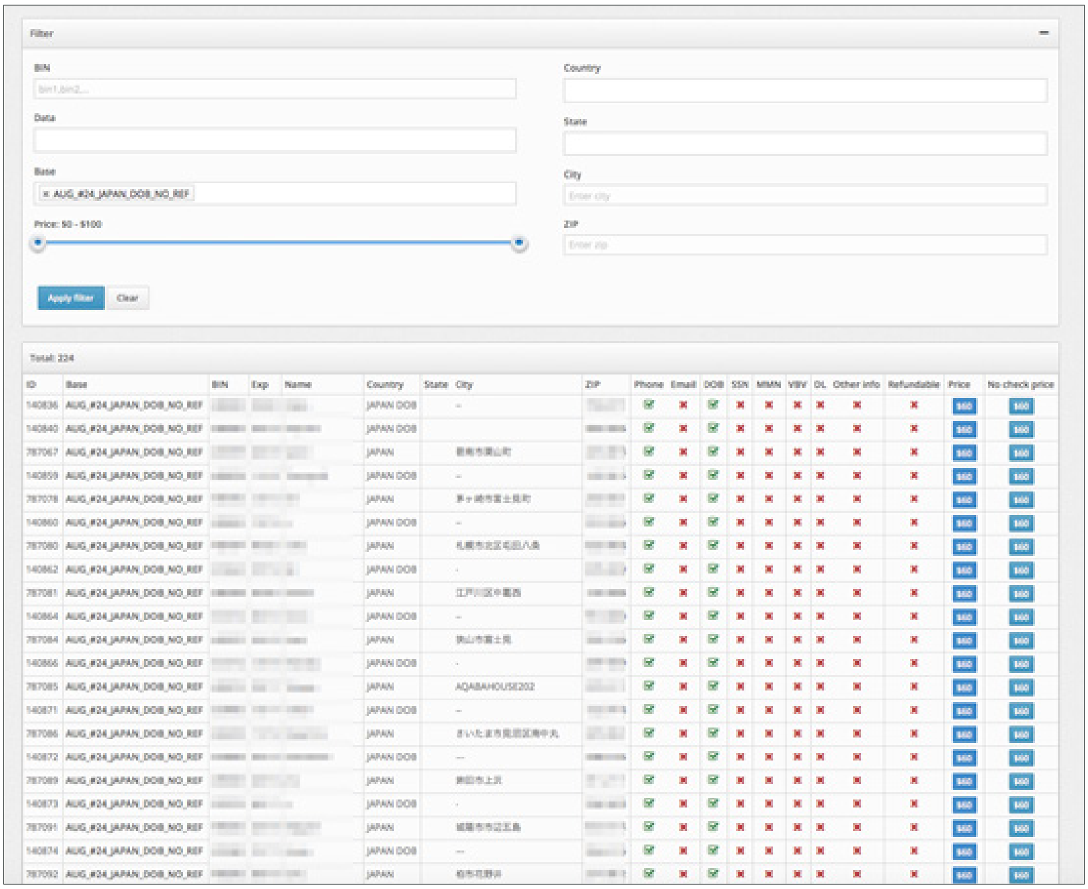
[redacted]

Figure 14: *Log-in page of JPON EXTREME, the most powerful search site for telephone numbers, according to its description; JPON EXTREME offers a total of 600 million telephone records collected since 1993*

Stolen account credentials and credit card validators

Another underground site, Orda Project (*http://[REDACTED]oej2qqacwz.onion/*), offers stolen account credentials to registered users. Various credit card, PayPal®, and Secure Shell (SSH) account credentials are sold at varying prices on the site.

Research revealed that Orda Project had three major price ranges. Stolen credit card credentials that cost US$60 or more include those for cards that have been verified by Visa™ via the Verified by Visa (VBV) service[19], which adds another security layer against unauthorized online use. There were more affordable offerings though. Incomplete and unverified credit card credentials were sold for US$10–59. Basic credentials, including owners' names, credit card numbers, and expiration dates, cost less than US$10.



Filter

BIN: bin1,bin2...

Data:

Base: × AUG_#24_JAPAN_DOB_NO_REF

Price: $0 - $100

Country:

State:

City: Enter city

ZIP: Enter zip

Apply filter | Clear

Total: 224

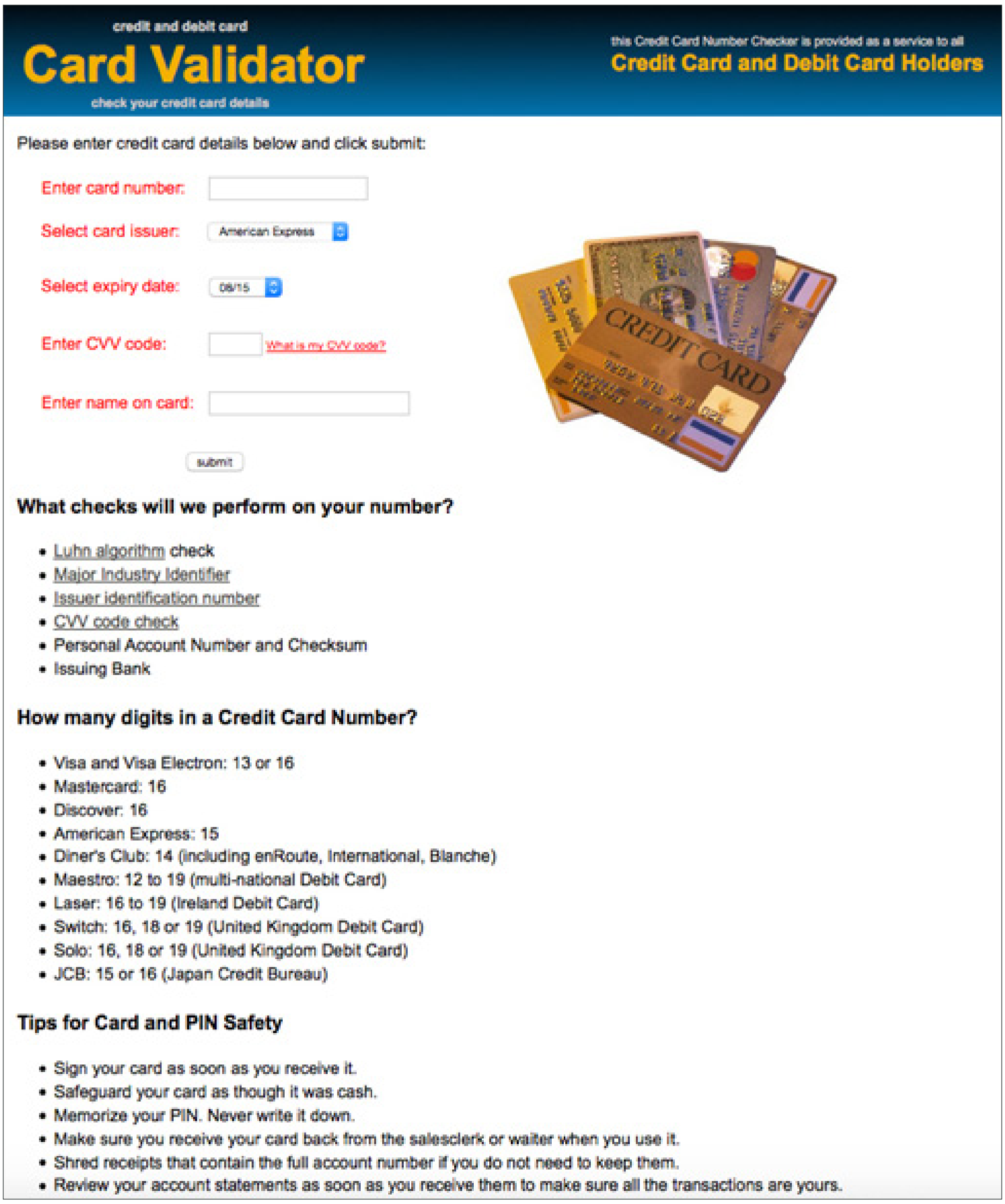
ID	Base	BIN	Exp	Name	Country	State	City	ZIP	Phone	Email	DOB	SSN	MMN	VBV	DL	Other info	Refundable	Price	No-check price
140836	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		–	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140840	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB			[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787067	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		[illegible]	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140859	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		–	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787078	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		茅ヶ崎市富士見町	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140860	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		–	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787080	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		札幌市北区屯田八条	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140862	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		-	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787081	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		江戸川区中葛西	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140864	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		–	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787084	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		狭山市富士見	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140866	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		-	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787085	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		AQABAHOUSE202	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140871	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		–	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787086	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		さいたま市見沼区南中丸	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140872	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		—	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787089	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		[illegible]	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140873	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		-	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787091	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		[illegible]	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
140874	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN DOB		—	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60
787092	AUG_#24_JAPAN_DOB_NO_REF	[redacted]	[redacted]	[redacted]	JAPAN		柏市花野井	[redacted]	✓	✗	✓	✗	✗	✗	✗	✗	✗	$60	$60

Figure 15: *List of credit card credentials sold on Orda Project*

Country	Selling price	Number of accounts for sale
	Credit cards	
Japan	US$14–78 (Average: ~US$60)	207
US	US$2–84 (Average: ~US$7)	126,707
Brazil	US$6–10 (Average: ~US$8)	17,385
UK	US$8–61 (Average: ~US$8)	28,336
Canada	US$3–60 (Average: ~US$16)	36,423
	PayPal accounts	
Japan	US$2	7
US	US$2	16,633
China	US$2	37
Brazil	US$2	83
UK	US$2	695
Canada	US$2	274
	SSH accounts	
Japan	US$1.40	1
US	US$1.40	1,186
Brazil	US$1.40	16
UK	US$1.40	25

Table 1: *Comparison of prices of stolen Japanese account credentials with those from other countries*

Credit card validators are also offered underground. These are illegal services used to check a credit card's validity. One such service, Card Validator, only works on one Japanese card brand, JCB.



credit and debit card

Card Validator

check your credit card details

this Credit Card Number Checker is provided as a service to all

Credit Card and Debit Card Holders

Please enter credit card details below and click submit:

Enter card number:

Select card issuer: American Express

Select expiry date: 08/15

Enter CVV code: What is my CVV code?

Enter name on card:

What checks will we perform on your number?

- Luhn algorithm check
- Major Industry Identifier
- Issuer identification number
- CVV code check
- Personal Account Number and Checksum
- Issuing Bank

How many digits in a Credit Card Number?

- Visa and Visa Electron: 13 or 16
- Mastercard: 16
- Discover: 16
- American Express: 15
- Diner's Club: 14 (including enRoute, International, Blanche)
- Maestro: 12 to 19 (multi-national Debit Card)
- Laser: 16 to 19 (Ireland Debit Card)
- Switch: 16, 18 or 19 (United Kingdom Debit Card)
- Solo: 16, 18 or 19 (United Kingdom Debit Card)
- JCB: 15 or 16 (Japan Credit Bureau)

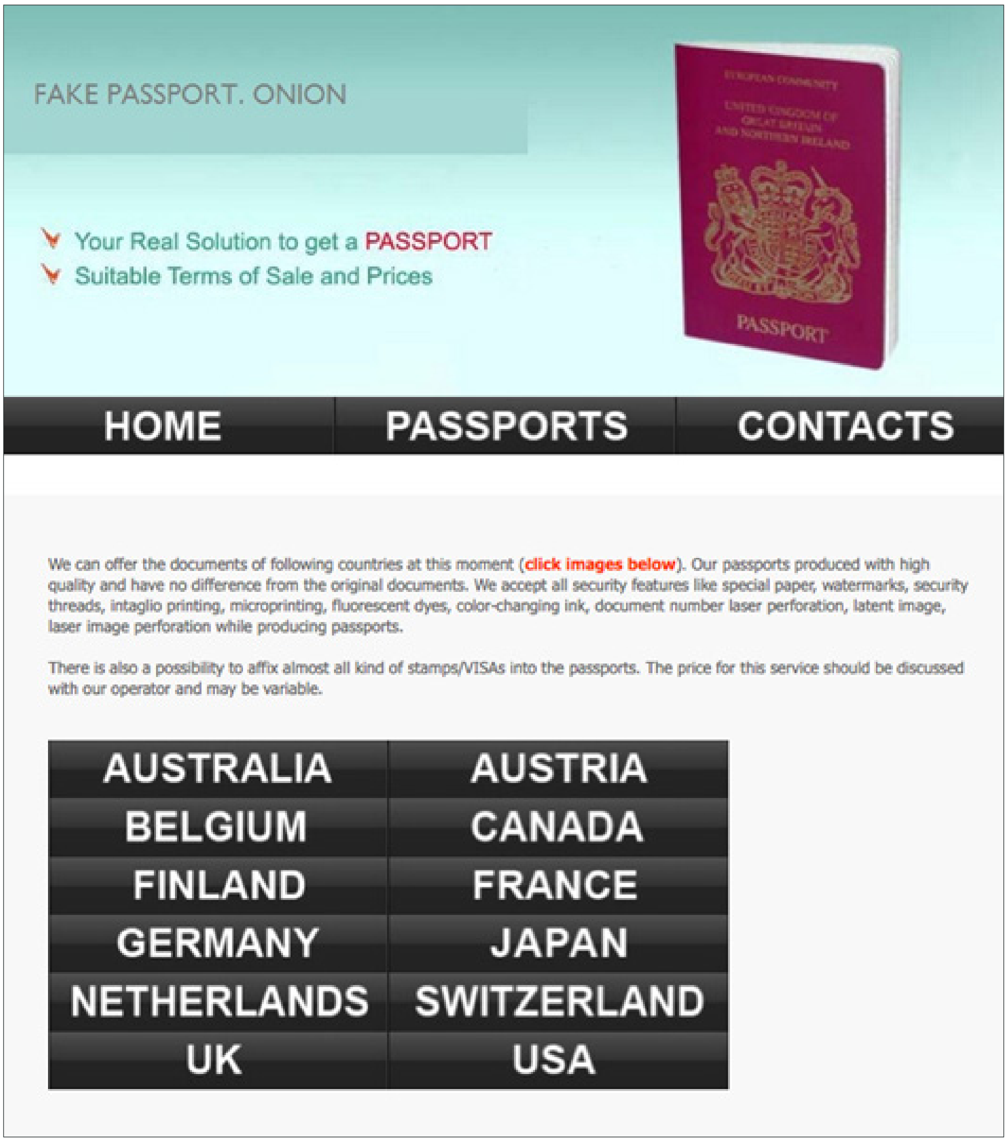
Tips for Card and PIN Safety

- Sign your card as soon as you receive it.
- Safeguard your card as though it was cash.
- Memorize your PIN. Never write it down.
- Make sure you receive your card back from the salesclerk or waiter when you use it.
- Shred receipts that contain the full account number if you do not need to keep them.
- Review your account statements as soon as you receive them to make sure all the transactions are yours.

Figure 16: *Card Validator's home page*

Fake passports

Fake passports, along with other forms of identification, are favored Deep Web commodities[20]. We found a counterfeit-passport shopping site called “FAKE PASSPORT.ONION,” that sells passports for 12 countries, including Japan.



FAKE PASSPORT. ONION

Your Real Solution to get a PASSPORT

Suitable Terms of Sale and Prices

We can offer the documents of following countries at this moment (click images below). Our passports produced with high quality and have no difference from the original documents. We accept all security features like special paper, watermarks, security threads, intaglio printing, microprinting, fluorescent dyes, color-changing ink, document number laser perforation, latent image, laser image perforation while producing passports.

There is also a possibility to affix almost all kind of stamps/VISAs into the passports. The price for this service should be discussed with our operator and may be variable.

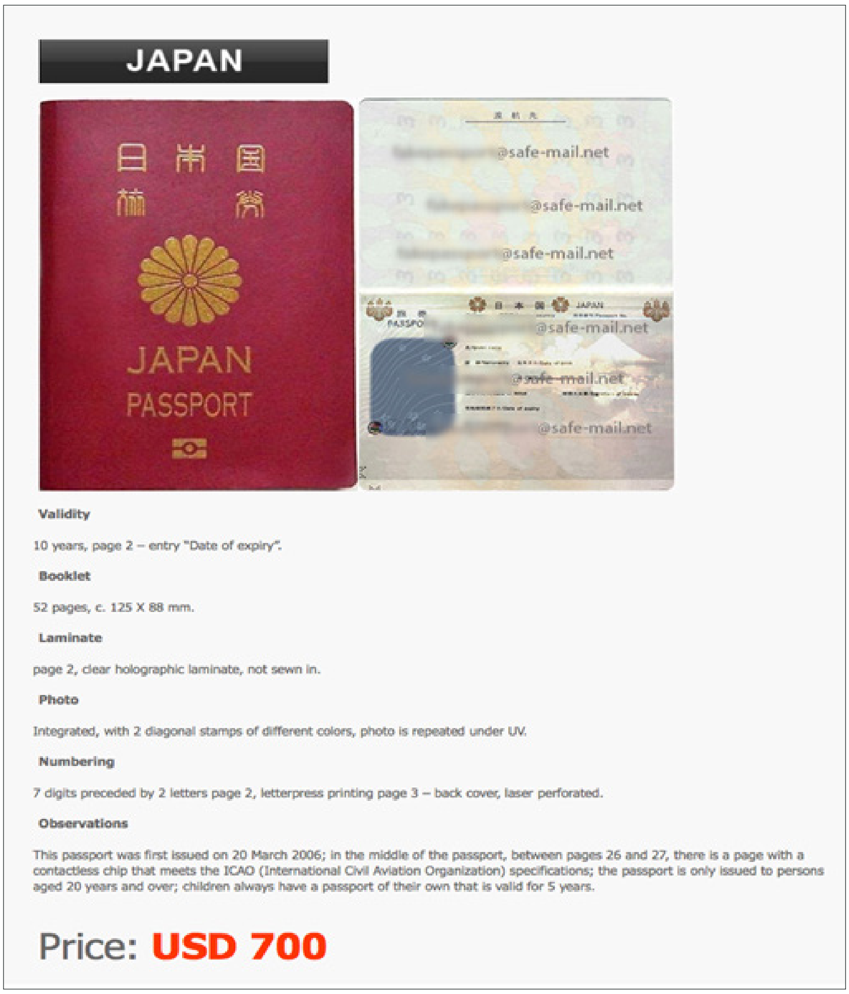
AUSTRALIA	AUSTRIA
BELGIUM	CANADA
FINLAND	FRANCE
GERMANY	JAPAN
NETHERLANDS	SWITZERLAND
UK	USA

Figure 17: *FAKE PASSPORT.ONION’s home page*

FAKE PASSPORT.ONION sells fake Japanese passports for US$700 each. US passports, meanwhile, fetched the highest price (US$1,000 each).

Country	Selling price
US	US$1,000
Switzerland	US$900
UK	US$900
Australia	US$850
Germany	US$850
Austria	US$800
Canada	US$800
France	US$800
Netherlands	US$800
Belgium	US$750
Finland	US$750
Japan	US$700

***Table 2:** Passports sold on FAKE PASSPORT.ONION with their prices*



JAPAN

Validity

10 years, page 2 – entry "Date of expiry".

Booklet

52 pages, c. 125 X 88 mm.

Laminate

page 2, clear holographic laminate, not sewn in.

Photo

Integrated, with 2 diagonal stamps of different colors, photo is repeated under UV.

Numbering

7 digits preceded by 2 letters page 2, letterpress printing page 3 – back cover, laser perforated.

Observations

This passport was first issued on 20 March 2006; in the middle of the passport, between pages 26 and 27, there is a page with a contactless chip that meets the ICAO (International Civil Aviation Organization) specifications; the passport is only issued to persons aged 20 years and over; children always have a passport of their own that is valid for 5 years.

Price: **USD 700**

***Figure 18:** Ad for Japanese passports sold underground*

Child pornography

Some Japanese underground sites serve as home to child pornography. Magical Onion is one such site. It serves as a trading platform for heinous content. Its registered users need to buy "magical points" to be able to exchange content with others. It only uses Japanese, which indicates that all of its members are either nationals or native speakers.

In 2014, Japan passed a law banning child pornography. As such, anyone in possession of related materials faces huge consequences, even imprisonment. Under this law, offenders found in possession of pornographic videos or photos of children can be fined up to ¥1 million (US$8,351)[21].

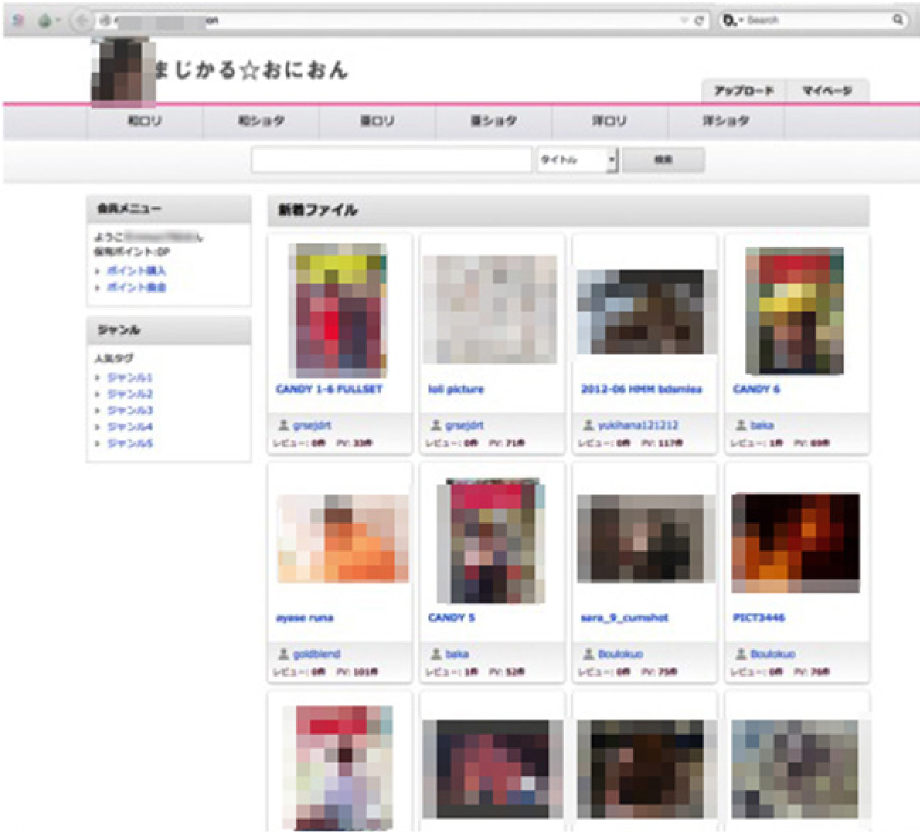
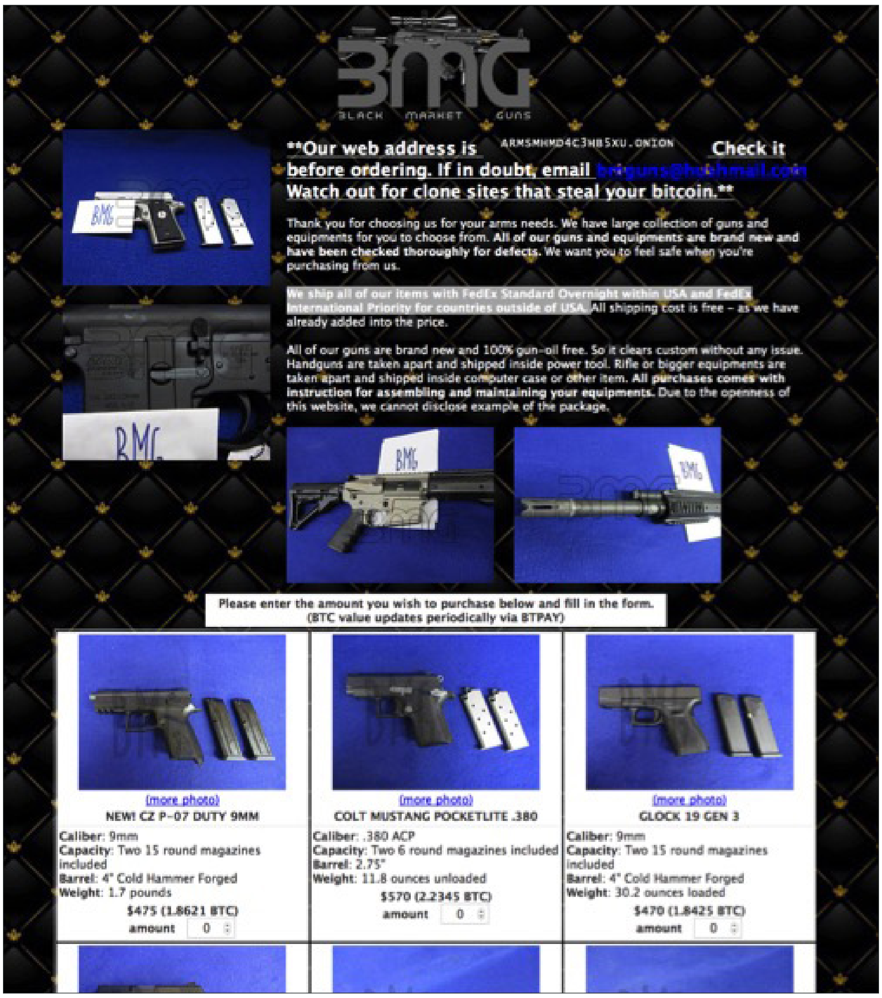


__Figure 19:__ Child porn traded on Magical Onion

Weapons

Just like any other place in the Dark Web, some Japanese underground sites also serve as weapon depots. Sites like Black Market Guns (BMG) have even eliminated middlemen between gun enthusiasts and dealers for those willing to purchase supposedly untraceable firearms.

BMG sells guns and ammunitions to buyers worldwide, hence the English text. It even claims to ship overnight to the US and other countries via FedEx.



Our web address is ARMSMHMD4C3HB5XU.ONION Check it before ordering. If in doubt, email bmguns@hushmail.com Watch out for clone sites that steal your bitcoin.

Thank you for choosing us for your arms needs. We have large collection of guns and equipments for you to choose from. **All of our guns and equipments are brand new and have been checked thoroughly for defects.** We want you to feel safe when you're purchasing from us.

We ship all of our items with FedEx Standard Overnight within USA and FedEx International Priority for countries outside of USA. All shipping cost is free – as we have already added into the price.

All of our guns are brand new and 100% gun-oil free. So it clears custom without any issue. Handguns are taken apart and shipped inside power tool. Rifle or bigger equipments are taken apart and shipped inside computer case or other item. **All purchases comes with instruction for assembling and maintaining your equipments.** Due to the openness of this website, we cannot disclose example of the package.

Please enter the amount you wish to purchase below and fill in the form.
(BTC value updates periodically via BTPAY)

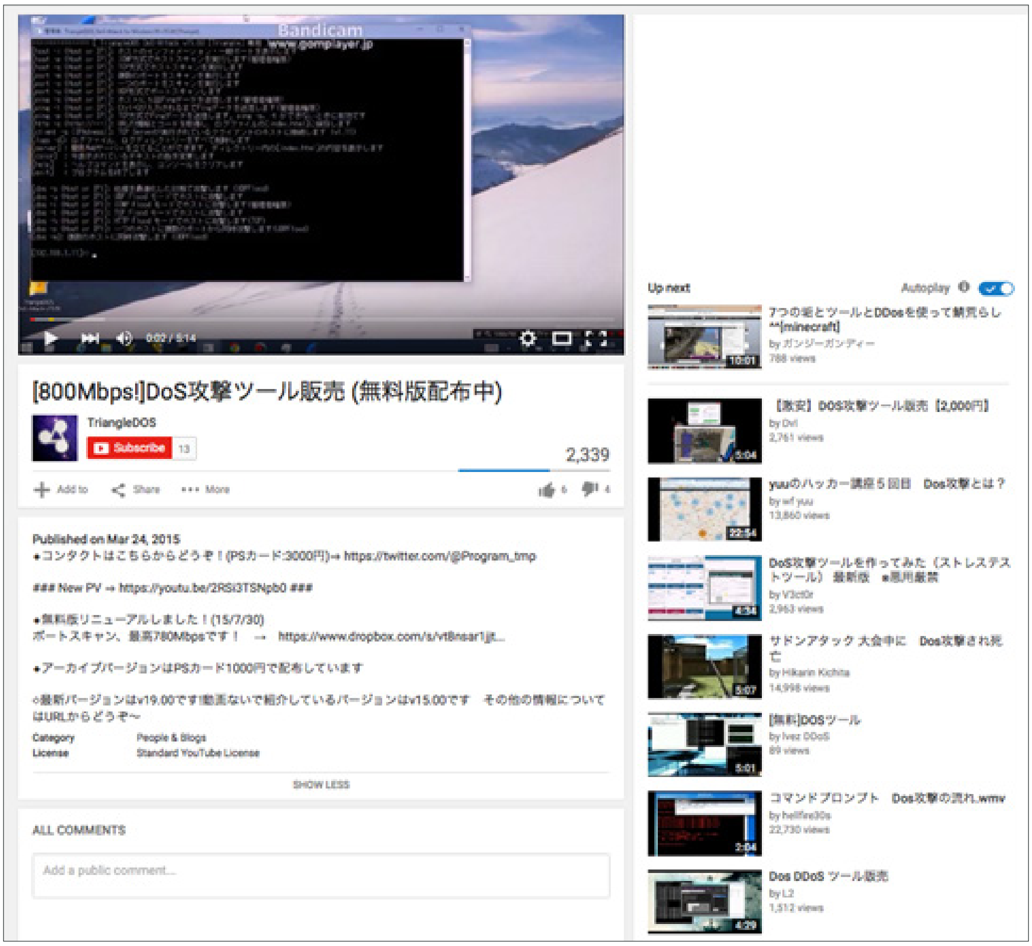
(more photo) NEW! CZ P-07 DUTY 9MM	(more photo) COLT MUSTANG POCKETLITE .380	(more photo) GLOCK 19 GEN 3
Caliber: 9mm **Capacity**: Two 15 round magazines included **Barrel**: 4" Cold Hammer Forged **Weight**: 1.7 pounds $475 (1.8621 BTC) amount 0	**Caliber**: .380 ACP **Capacity**: Two 6 round magazines included **Barrel**: 2.75" **Weight**: 11.8 ounces unloaded $570 (2.2345 BTC) amount 0	**Caliber**: 9mm **Capacity**: Two 15 round magazines included **Barrel**: 4" Cold Hammer Forged **Weight**: 30.2 ounces loaded $470 (1.8425 BTC) amount 0

Figure 20: *BMG's home page*

Hacking knowledge

The Japanese underground market not only offers goods, but also hacking advice. Users can get tips on hacking enemies, extorting money using malware, and where to get the tools they would need.

We also found a site (likely owned by a Japanese) that offers a denial-of-service (DoS) tool. DoS tools can not only be used in cyber attacks, but also for testing load balancers. He owns the TriangleDOS account on YouTube™ and goes by the handle, Program_tmp, on Twitter. He offers a tool called "TriangleDOS v16.10" to anyone interested. While cybercriminals or malicious tool developers often ask for money in exchange for services rendered, TriangleDOS does not. He instead asks for PlayStation Store cards worth ¥1,000–3,000 (US$8.35–25.05) as payment.



[800Mbps!]DoS攻撃ツール販売 (無料版配布中)

TriangleDOS

Subscribe 13

2,339

Published on Mar 24, 2015

●コンタクトはこちらからどうぞ！(PSカード:3000円)→ https://twitter.com/@Program_tmp

New PV → https://youtu.be/2RSi3TSNpb0

●無料版リニューアルしました！(15/7/30)
ポートスキャン、最高780Mbpsです！ → https://www.dropbox.com/s/vt8nsar1jjt...

●アーカイブバージョンはPSカード1000円で配布しています

○最新バージョンはv19.00です!動画ないで紹介しているバージョンはv15.00です　その他の情報についてはURLからどうぞ〜

Category　People & Blogs
License　Standard YouTube License

7つの砦とツールとDDosを使って鯖荒らし^^[minecraft]
by ガンジーガンディー
788 views

【激安】DOS攻撃ツール販売【2,000円】
by Dvl
2,761 views

yuuのハッカー講座５回目　Dos攻撃とは？
by wf yuu
13,860 views

DoS攻撃ツールを作ってみた（ストレステストツール）最新版　※悪用厳禁
by V3ct0r
2,963 views

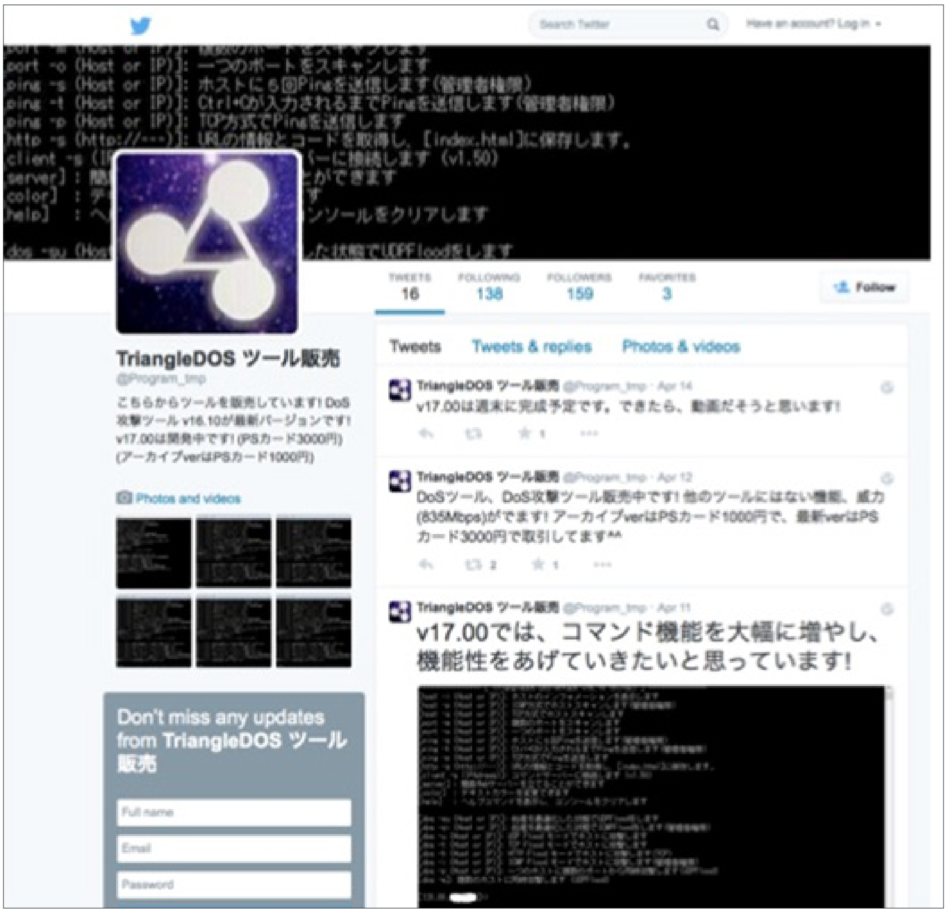
サドンアタック 大会中に　Dos攻撃され死亡
by Hikaru Kichita
14,998 views

[無料]DOSツール
by Ivez DDoS
89 views

コマンドプロンプト　Dos攻撃の流れ.wmv
by hellfire30s
22,730 views

Dos DDoS ツール販売
by L2
1,512 views

Figure 21: *TriangleDOS's sales video on YouTube with a download link*



```
port -m (Host or IP)]: 複数のポートをスキャンします
port -o (Host or IP)]: 一つのポートをスキャンします
ping -s (Host or IP)]: ホストに5回Pingを送信します(管理者権限)
ping -t (Host or IP)]: Ctrl+Cが入力されるまでPingを送信します(管理者権限)
ping -p (Host or IP)]: TCP方式でPingを送信します
http -s (http://---)]: URLの情報とコードを取得し、[index.html]に保存します。
client -s (I                ーに接続します (v1.50)
server] : 簡                とができます
color]  : デ                す
help]   : ヘ                ンソールをクリアします

dos -su (Host               した状態でUDPFloodをします
```

TriangleDOS ツール販売
@Program_tmp

こちらからツールを販売しています! DoS攻撃ツール v16.10が最新バージョンです! v17.00は開発中です! (PSカード3000円) (アーカイブverはPSカード1000円)

TriangleDOS ツール販売 @Program_tmp · Apr 14
v17.00は週末に完成予定です。できたら、動画だそうと思います!

TriangleDOS ツール販売 @Program_tmp · Apr 12
DoSツール、DoS攻撃ツール販売中です! 他のツールにはない機能、威力(835Mbps)がでます! アーカイブverはPSカード1000円で、最新verはPSカード3000円で取引してます^^

TriangleDOS ツール販売 @Program_tmp · Apr 11
v17.00では、コマンド機能を大幅に増やし、機能性をあげていきたいと思っています!

Don't miss any updates from TriangleDOS ツール販売

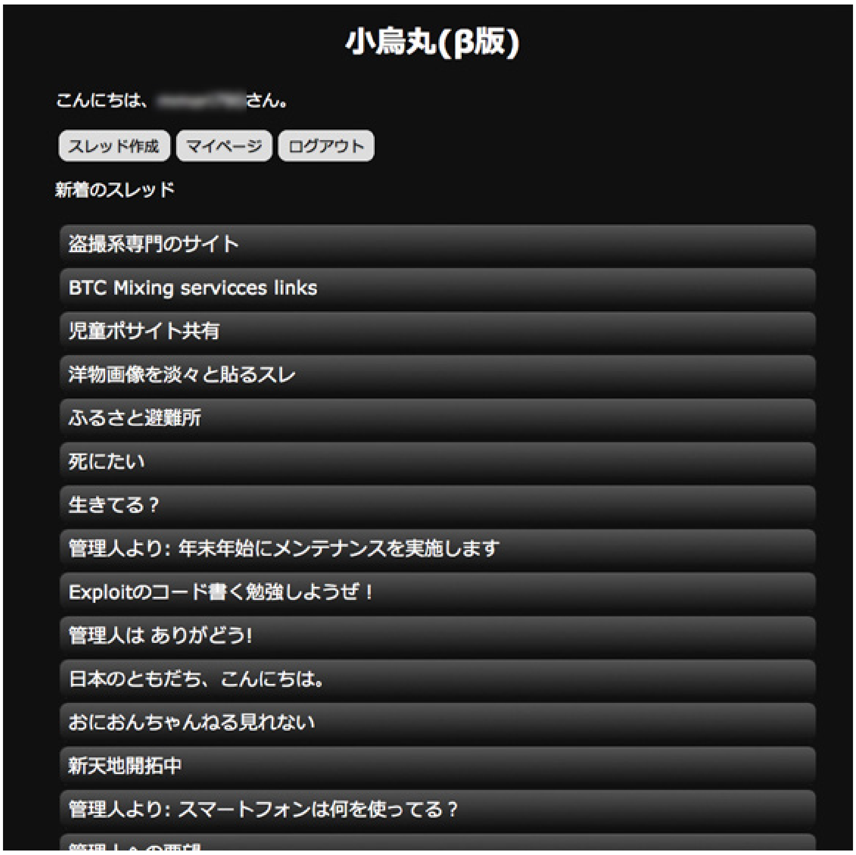
Full name

Email

Password

Figure 22: *TriangleDOS's tweets related to selling his malicious tool, an older version of which costs ¥1,000 or US$8.35 while a newer one costs ¥3,000 or US$25.05; his Twitter account description gives updates on his DoS attack tool (v16.10 is the latest version and v17.0 is currently being developed)*

We also found Kogarasu-maru, another venue where hackers can share with and gain knowledge from their peers. The forum covers a wide range of topics, ranging from child porn to writing exploit codes.



小烏丸(β版)

こんにちは、[redacted]さん。

スレッド作成 | マイページ | ログアウト

新着のスレッド

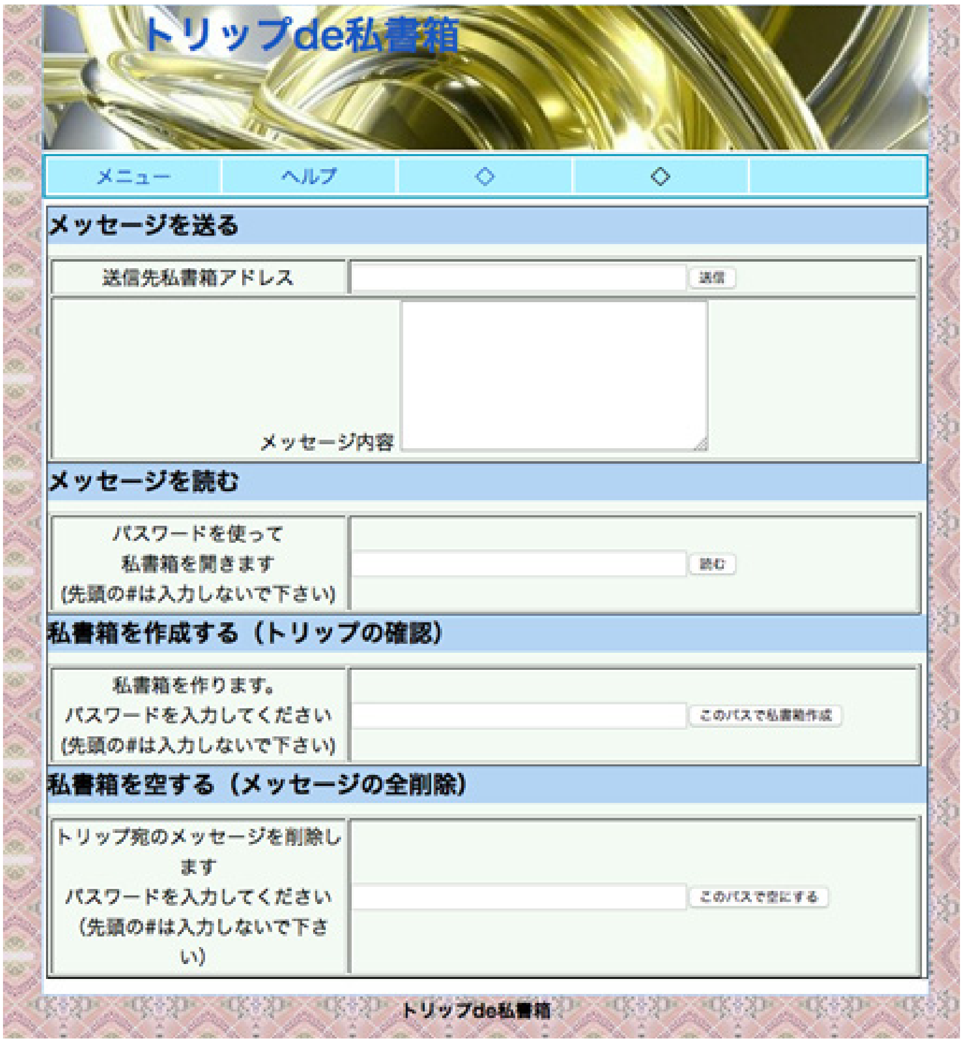
- 盗撮系専門のサイト
- BTC Mixing servicces links
- 児童ポサイト共有
- 洋物画像を淡々と貼るスレ
- ふるさと避難所
- 死にたい
- 生きてる？
- 管理人より: 年末年始にメンテナンスを実施します
- Exploitのコード書く勉強しようぜ！
- 管理人は ありがどう!
- 日本のともだち、こんにちは。
- おにおんちゃんねる見れない
- 新天地開拓中
- 管理人より: スマートフォンは何を使ってる？
- 管理人への要望

Figure 23: *Kogarasu-maru’s various users offer hidden camera services (盗撮系専門のサイト), exploit-creation (Exploitのコード書く勉強しようぜ！) and TOR access tutorials (おにおんちゃんねる見れない); share bitcoin-mixing-service links and child porn (児童ポサイト共有); and receive messages from the site administrator (管理人より), along with invitations from co-users to commit group suicide (死にたい)*

Virtual PO boxes

Another means by which hacking information is shared is via virtual PO boxes. Apart from SAFe-mail and Extensible Messaging and Presence Protocol (XMPP), virtual PO boxes also allow hackers to anonymously share information with one another.

We also saw underground sites that offer virtual PO boxes. Virtual PO boxes allow senders to generate unique addresses that they can send to receivers prior to using the messaging service. That way, they can anonymously exchange information with each other.



メッセージを送る

送信先私書箱アドレス

メッセージ内容

メッセージを読む

パスワードを使って
私書箱を開きます
(先頭の#は入力しないで下さい)

私書箱を作成する（トリップの確認）

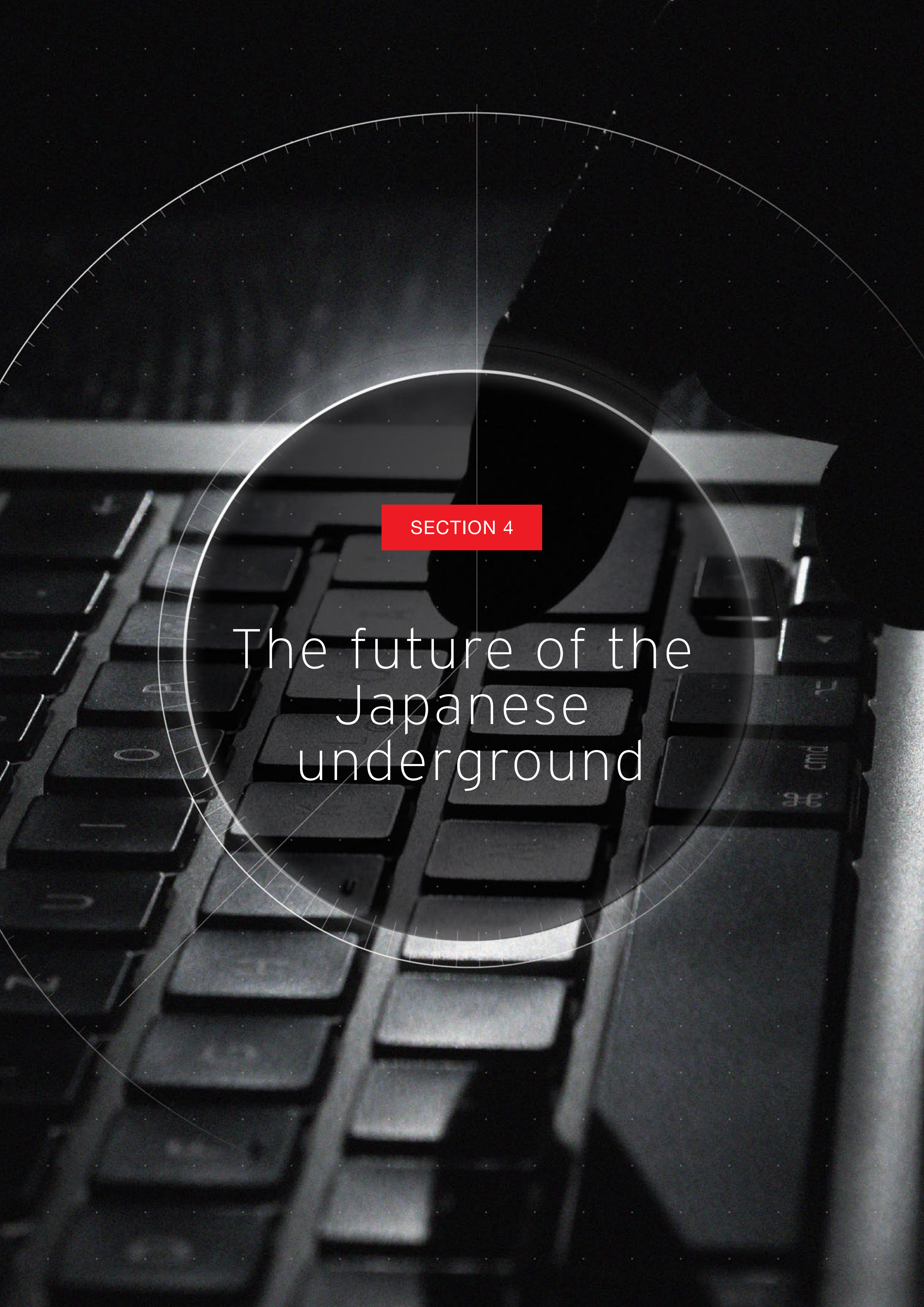
私書箱を作ります。
パスワードを入力してください
(先頭の#は入力しないで下さい)

私書箱を空する（メッセージの全削除）

トリップ宛のメッセージを削除します
パスワードを入力してください
（先頭の#は入力しないで下さい）

トリップde私書箱

***Figure 24:** Sample virtual-PO-box-messaging system where users can anonymously send messages to and receive responses from their underground peers; senders only need to input their messages and recipients' PO box addresses; recipients just need to enter their passwords in order to read messages*



SECTION 4

The future of the Japanese underground

The future of the Japanese underground

Japan's presence in the global cybercriminal underground, although still fairly small, is not negligible. We are seeing Japanese-speaking individuals converge into active communities on several underground BBSs. These forums, typically used to foster anonymous conversations on taboo topics, are turning into viable trading posts for prohibited goods and contraband. The way these boards are currently set up is reminiscent of Silk Road before it became a notorious marketplace[22].

Although our observations reveal that Japanese cybercriminals lack the technical know-how needed for malware creation, the interest is there, as evidenced by exchanges on how to monetize malware tools purchased from other regional underground markets. Once enterprising individuals discover the feasibility of making money using hacking or malware, we may see more locally produced hacking tools and tips on Japanese underground sites.

Japanese law enforcement agencies are making great strides in protecting their citizens against organized crime, but their efforts may also push criminals to go underground. Since there is pressure from the law that hinders bad guys from making money out of traditional schemes, they can opt to move their operations where legislation may be more lenient and attribution for their crimes, more difficult. If ever organized crime groups like the Yakuza ever venture into darknets, all they would need is the aid of tech-savvy individuals to engage in criminal transactions.

The Japanese cybercriminal underground is still young, and its future is wide open. Both law enforcement agencies and cybercriminals have yet to actively take advantage of this window of opportunity. Whoever does so first many gain an upper hand in the long run.

References

1. Maxim Goncharov. (28 July 2015). *TrendLabs Security Intelligence Blog*. "The Russian Underground—Revamped." Last accessed on 17 September 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-russian-underground-revamped/.

2. Fernando Mercês. (18 November 2014). *TrendLabs Security Intelligence Blog*. "Localized Tools and Services, Prominent in the Brazilian Underground." Last accessed on 17 September 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/localized-tools-and-services-prominent-in-the-brazilian-underground/.

3. Lion Gu. (13 November 2014). *TrendLabs Security Intelligence Blog*. "Tracking Activity in the Chinese Mobile Underground." Last accessed on 17 September 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/tracking-activity-in-the-chinese-mobile-underground/.

4. Miniwatts Marketing Group. (2001–2015). *Internet World Stats: Usage and Population Statistics.* "Internet Usage in Asia: Internet Users, Facebook Subscribers, and Population Statistics for 35 Countries and Regions in Asia." Last accessed on 17 September 2015, http://www.internetworldstats.com/stats3.htm.

5. Jiji Kyodo. (12 March 2015). *The Japan Times.* "Police Receive Record Number of Queries on Cybercrime." Last accessed on 17 September 2015, http://www.japantimes.co.jp/news/2015/03/12/national/crime-legal/police-receive-record-number-of-queries-on-cybercrime/#.VegdtyWqpHx.

6. Kyodo. (3 September 2015). *The Japan Times.* "Online Fraud Robs Japan Banks of ¥1.5 Billion in First Half of 2015." Last accessed on 17 September 2015, http://www.japantimes.co.jp/news/2015/09/03/national/crime-legal/online-fraud-robs-japan-banks-%C2%A51-5-billion-first-half-2015/#.VekRPCWqpHw.

7. Jonathan Leopando. (2 June 2014). *TrendLabs Security Intelligence Blog*. "Banking Trojan Trend Hits Japan Hard." Last accessed on 17 September 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/banking-trojan-trend-hits-japan-hard/.

8. TrendLabs. (2015). *Trend Micro Security Intelligence*. "A Rising Tide: New Hacks Threaten Public Technologies." Last accessed on 17 September 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_a_rising_tide.pdf.

9. Reuters. (1 June 2015). *The Asahi Shimbun*. "Japan Pension System Hacked, 1.25 Million Cases of Personal Data Leaked." Last accessed on 17 September 2015, http://ajw.asahi.com/article/behind_news/social_affairs/AJ201506010096.

10. TechTarget. (September 2005). *WhatIs.com.* "Bulletin board system (BBS)." Last accessed on 17 September 2015, http://whatis.techtarget.com/definition/bulletin-board-system-BBS.

11. Lisa Katayama. (19 April 2007). *Wired.* "2channel Gives Japan's Famously Quiet People a Mighty Voice." Last accessed on 17 September 2015, http://archive.wired.com/culture/lifestyle/news/2007/04/2channel.

12. Phil Muncaster. (13 February 2014). *The Register.* "'Demon Killer' Who Tied SD Card to Cat Pleads Not Guilty: Japanese Hacker Also Threatened to Blow Up Schools, Planes, Distributed Viruses." Last accessed on 17 September 2015, http://www.theregister.co.uk/2014/02/13/japan_cat_hacker_demon_killer_trial/.

13. BBC. (22 April 2013). *BBC News.* "Japanese Police Target Users of Tor Anonymous Network." Last accessed on 17 September 2015, http://www.bbc.com/news/technology-22248692.

14. *SAFe-mail.* Last accessed on 18 September 2015, https://www.safe-mail.net.

15. Using." Last accessed on 18 September 2015, http://www.forbes.com/sites/runasandvik/2014/01/31/the-email-service-the-dark-web-is-actually-using/.

16. Symantec Security Response. (15 December 2014). *Symantec Connect*. "TorLocker Ransomware Variant Designed to Target Japanese Users." Last accessed on 18 September 2015, http://www.symantec.com/connect/blogs/torlocker-ransomware-variant-designed-target-japanese-users.

17. Bun Wong. (1 July 2015). *Netease International News.* "Japanese 17-Year-Old on Suspicion of Making Japan's First 'Abduction Virus' Arrested." Last accessed on 18 September 2015, http://www.inews163.com/2015/07/01/japanese-17-year-old-on-suspicion-of-making-japans-first-abduction-virus-arrested-130201.html.

18. Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler. (2015). *Trend Micro Security Intelligence*. "Below the Surface: Exploring the Deep Web." Last accessed on 18 September 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf.

19. Visa. (1996—2015). *VISA*. "Security + Support." Last accessed on 23 September 2015, https://usa.visa.com/support/consumer/security.html/security-program/verified-by-visa.jsp.

20. Vincenzo Ciancaglini. (22 June 2015). *TrendLabs Security Intelligence Blog*. "Digging into the Deep Web." Last accessed on 18 September 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/digging-into-the-deep-web/.

21. Melissa Hellmann. (18 June 2014). *Time.* "Japan Finally Bans Child Pornography." Last accessed on 18 September 2015, http://time.com/2892728/japan-finally-bans-child-pornography/.

22. Robert McArdle. (3 October 2013). *TrendLabs Security Intelligence Blog*. "Deep Web and Cybercrime—It Is Not Just the Silk Road." Last accessed on 18 September 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/deepweb-and-cybercrime-it-is-not-just-the-silk-road/.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey
to the Cloud