The Japanese Underground

Akira Urano
Forward-Looking Threat Research (FTR) Team

A TrendLabs™ Research Paper
Contents

4
Cybercrime in Japan

6
Bulletin board systems: Forging anonymity

15
Japanese underground market offerings

30
The future of the Japanese underground
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, Brazil, and China.
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, 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 while the total estimated online fraud damage cost banks ¥1.54 billion or US$13 million in the first half of 2015. 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. As of the second quarter of this year, the country was also most affected by Angler-Exploit-Kit-related activity (49%).

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. 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).
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. 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.

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. Katayama was also eventually arrested in February 2013.

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

Figure 3: CAPTCHA that asks visitors of Magical Onion, a child porn site, to enter Hiragana characters (ないまこぼ) 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.

![Fake welcome page with clickable flags that lead to the real Tor 2 Channel page](image)

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

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.

Figure 5: SAFe-mail’s sign-up form
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)

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 0chiaki

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, attempted hacking, and credit card fraud, among other crimes.

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.

Figure 8: Koushin Underground’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)
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

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つくのは)
SECTION 3

Japanese underground market offerings
Japanese underground market offerings

We used an internally developed system called “Deep Web Analyzer” 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.
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.

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.)

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) service19, 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.

Figure 15: List of credit card credentials sold on Orda Project
<table>
<thead>
<tr>
<th>Country</th>
<th>Selling price</th>
<th>Number of accounts for sale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credit cards</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>US$14–78 (Average: ~US$60)</td>
<td>207</td>
</tr>
<tr>
<td>US</td>
<td>US$2–84 (Average: ~US$7)</td>
<td>126,707</td>
</tr>
<tr>
<td>Brazil</td>
<td>US$6–10 (Average: ~US$8)</td>
<td>17,385</td>
</tr>
<tr>
<td>UK</td>
<td>US$8–61 (Average: ~US$8)</td>
<td>28,336</td>
</tr>
<tr>
<td>Canada</td>
<td>US$3–60 (Average: ~US$16)</td>
<td>36,423</td>
</tr>
<tr>
<td><strong>PayPal accounts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>US$2</td>
<td>7</td>
</tr>
<tr>
<td>US</td>
<td>US$2</td>
<td>16,633</td>
</tr>
<tr>
<td>China</td>
<td>US$2</td>
<td>37</td>
</tr>
<tr>
<td>Brazil</td>
<td>US$2</td>
<td>83</td>
</tr>
<tr>
<td>UK</td>
<td>US$2</td>
<td>695</td>
</tr>
<tr>
<td>Canada</td>
<td>US$2</td>
<td>274</td>
</tr>
<tr>
<td><strong>SSH accounts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>US$1.40</td>
<td>1</td>
</tr>
<tr>
<td>US</td>
<td>US$1.40</td>
<td>1,186</td>
</tr>
<tr>
<td>Brazil</td>
<td>US$1.40</td>
<td>16</td>
</tr>
<tr>
<td>UK</td>
<td>US$1.40</td>
<td>25</td>
</tr>
</tbody>
</table>

**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.
Figure 16: Card Validator’s home page
Fake passports

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

![Figure 17: FAKE PASSPORT.ONION's home page](image)

FAKE PASSPORT.ONION sells fake Japanese passports for US$700 each. US passports, meanwhile, fetched the highest price (US$1,000 each).
<table>
<thead>
<tr>
<th>Country</th>
<th>Selling price</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>US$1,000</td>
</tr>
<tr>
<td>Switzerland</td>
<td>US$900</td>
</tr>
<tr>
<td>UK</td>
<td>US$900</td>
</tr>
<tr>
<td>Australia</td>
<td>US$850</td>
</tr>
<tr>
<td>Germany</td>
<td>US$850</td>
</tr>
<tr>
<td>Austria</td>
<td>US$800</td>
</tr>
<tr>
<td>Canada</td>
<td>US$800</td>
</tr>
<tr>
<td>France</td>
<td>US$800</td>
</tr>
<tr>
<td>Netherlands</td>
<td>US$800</td>
</tr>
<tr>
<td>Belgium</td>
<td>US$750</td>
</tr>
<tr>
<td>Finland</td>
<td>US$750</td>
</tr>
<tr>
<td>Japan</td>
<td>US$700</td>
</tr>
</tbody>
</table>

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

*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).
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 ammunition to buyers worldwide, hence the English text. It even claims to ship overnight to the US and other countries via FedEx.

![Figure 20: BMG's home page](image)

**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.

Figure 21: TriangleDOS’s sales video on YouTube with a download link
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.
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.

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 marketplace22.

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


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 top-ranked 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.