JC3 Japan Cybercrime Control Center

APWG

Revealed Threat of Fake Store

Proposed New Definition of Fake Store

Published: June 5, 2018
Publisher: Japan Cybercrime Control Center (JC3) and Anti-Phishing Working Group (APWG)

Contents

1. Executive Summary

The APWG has two primary criteria that define a phishing website.

- Site mimics or impersonates a legitimate business or service
- Site collects sensitive financial or personal information (password, credit card number, etc.)

Nevertheless, “Fake Store” websites, that don’t meet the above criteria have caused considerable damage in Japan while posing as legitimate online shopping services. Criminals have been consistently operating them for stealing money and sensitive information.

Japan Cybercrime Control Center (JC3), which promotes public-private partnership for cyber security in Japan, researched approximately 7,000 websites reported to Police from June 2016 to June 2017 from victims who had money or sensitive information stolen, and figured out that most of them were ‘Fake Stores’, built by criminals, with the appearance of looking like ordinary online shopping websites.

As a proactive approach to defeat “Fake Store” websites, JC3 has been seeking to comprehensively identify all of the “Fake Stores” by analyzing criminals’ modus operandi. This is possible because they have been making many “Fake Store” websites in a similar way. Most of them are not yet recognized as fraudulent websites, but they will soon victimize individuals.

The characteristics of “Fake Store” JC3 identified by JC3’s analysis are as below.

Type	Characteristics of Fake Store	Criminal Group
Type 1	Embedded code into a compromised website redirects users to a “Fake Store” website	Group A/D/E/F
Type 2	Fake Store website frequently changes its company profile weekly, monthly, or each time an IP address is changed in order to deceive users	Group B
Type 3	Fake Store has non-existent or fake company profiles instead of legitimate company profiles*	Group C

* A legitimate company profile is required, by law in Japan, for an online shopping website.

This white paper provides details of the “Fake Store” threat, as revealed by the latest research.

In the near future, it is expected that APWG should set a new definition of a “Fake Store” as a harmful threat for users and a security alert should be popped up on browser or endpoint security software for prevention of damage.

As cyber criminals are not targeting a specific country or language, we hope this white paper will contribute to reduce victims of “Fake Store” websites for APWG members and others that do not recognize the threat.

2. Current Situation on Phishing Websites

While APWG and law enforcement have been developing countermeasures against phishing websites, “Fake Store” sites have caused significant damage in Japan.

2.1 Countermeasures against Phishing website

The APWG has two primary criteria that define a phishing website.

- Site mimics or impersonates a legitimate business or service
- Site collects sensitive financial or personal information (password, credit card number, etc.)

Based on these criteria, APWG and related organizations have been cooperating in global efforts to detect and mitigate phishing websites.

2.2 Victims of “Fake Store” in Japan

Nevertheless, “Fake Store” websites, that don’t meet the above criteria have caused considerable damage in Japan while posing as legitimate online shopping services. Criminals have been consistently operating them for stealing money and sensitive information.

2.2.1 Increasing Number of Cybercrime Complaints in Japan

The Japanese Police received 131,518 complaints or reports about cybercrime from victims in 2016. Compared to the 77,815 complaints received in 2012, it has been increasing year by year in Japan.

Complaints or reports about fraudulent or counterfeit websites account for 40 to 60 percent of the total number of complaints, which have more than doubled in the past five years.

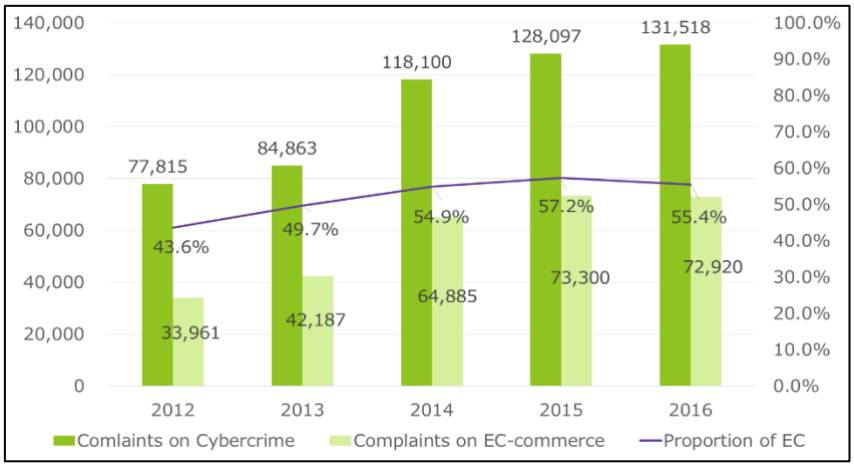

Figure 1: Number of Cybercrime Complaints Reported to Police in Japan

The two most common complaints about fraudulent or counterfeit websites are;

- I have received nothing, even after payment on an online shopping website.
- Despite entering credit card information, I could not complete the payment on an online shopping website.

While these "Fake Store" websites don't meet the above APWG's criteria, they have caused considerable damage resulting in the theft of money and sensitive information in Japan. Criminals have been consistently operating storefronts that pose as legitimate online shopping services.

According to the press release, Police confirmed that criminals have received at least 240 million yen ($2.1 million) between May and December of 2017 by investigating bank accounts designated by "Fake Store" websites for payment[1]. It is assumed to be just the tip of the iceberg regarding overall damage from "Fake Stores".

2.2.2 Countermeasures against malicious websites by Japanese Police

Although the number of complaints or reports to Japanese Police about fraudulent or counterfeit or phishing websites is increasing, Japanese Police have faced difficulty when they directly investigate overseas servers used for criminals' activities or overseas administrators of the websites.

In response to this lack of support, the National Police Agency (NPA) has been collecting the domain names of overseas malicious websites, in particular from police nationwide that receive complaints or reports from victims who had money or sensitive information stolen, in order to provide that information to antivirus vendors and security vendors. The request to these vendors encourages them to provide security alerts within their software to help prevent the damage incurred when users view these websites.

Since June 2016, NPA has been providing APWG with the list of overseas malicious websites domain names provided by victims with actual damage and some APWG member companies use them for their security alerts.

[1] Refer to the article on 21th of December 2017 from the Mainichi Newspapers (https://mainichi.jp/articles/20171221/dde/041/040/029000c) or from the Japan Times (https://www.japantimes.co.jp/news/2017/12/21/national/cybersecurity-survey-japan-finds-20000-fake-shopping-sites/).

3. JC3's Analysis of Fake Store

Japan Cybercrime Control Center (JC3) has analyzed the characteristics of "Fake Stores".

3.1 Fake Store Reported from Victims

JC3, which promotes public-private partnership for cyber security in Japan, researched approximately 7,000 malicious websites reported to Police from June 2016 to June 2017 from victims that reported stolen money or sensitive information[2].

As a result, while few of them were phishing websites that met the APWG's criteria, JC3 discovered that 87% of them were "Fake Stores" that pose as ordinary online shopping websites. These storefronts have been operated by criminals for the purpose of stealing money and sensitive information (See Figure 2).

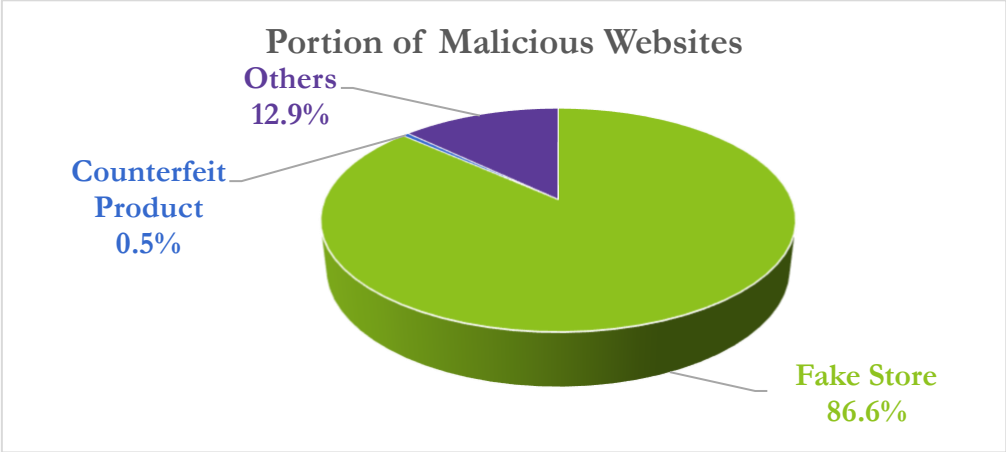

Figure 2: Classification of the Malicious Websites Reported to Police

3.2 Analysis of Characteristics of Fake Store

Yet "Fake Stores" artfully pose as ordinary online shopping websites. JC3's analysis shows that they have distinctive characteristics legitimate online shopping websites never have.

Every "Fake Store" JC3 found, has at least one of the following three characteristics[3].

- Type 1: Embedded code in a compromised website redirects users to a "Fake Store" website
- Type 2: A "Fake Store" website frequently changes its company profile each time an IP address is changed in an attempt to deceive users

[2] Refer to appendix (7.1 Research Items of Malicious Websites).
[3] Refer to appendix (7.2 Detail of Characteristics of "Fake Stores").

- Type 3: “Fake Store” has no legitimate company profiles or a fake company profiles*
  * A legitimate company profile is required, by law in Japan, for an online shopping website.

A lot of users seem to believe “Fake Stores” to be legitimate when they view them because “Fake Stores” use images and contents of legitimate online shopping websites without permission, and moreover, they have an abundance of products sold at cheaper price than the legitimate online shopping website price. Many victims have paid their money into bank accounts “Fake Stores” gave them and sent their personal information including card numbers to these “Fake Stores” without knowing it was a scam.

3.2.1 Type 1: Redirecting users through a compromised website

Criminal groups have compromised legitimate websites to embed code that supports “Fake Stores” appearing higher in search results, which seems to deceive users and induce them to click their “Fake Stores” through the compromised websites. When a user searches a product for their purchase, some compromised websites appear high in the search results, because criminal groups have so good skill in SEO to pass attractive product information to web crawling bots. If the user clicks the link to one of them, the embedded code in the compromised website automatically redirects him/her to a “Fake Store” website and displays it on their screen (See Figure 3).

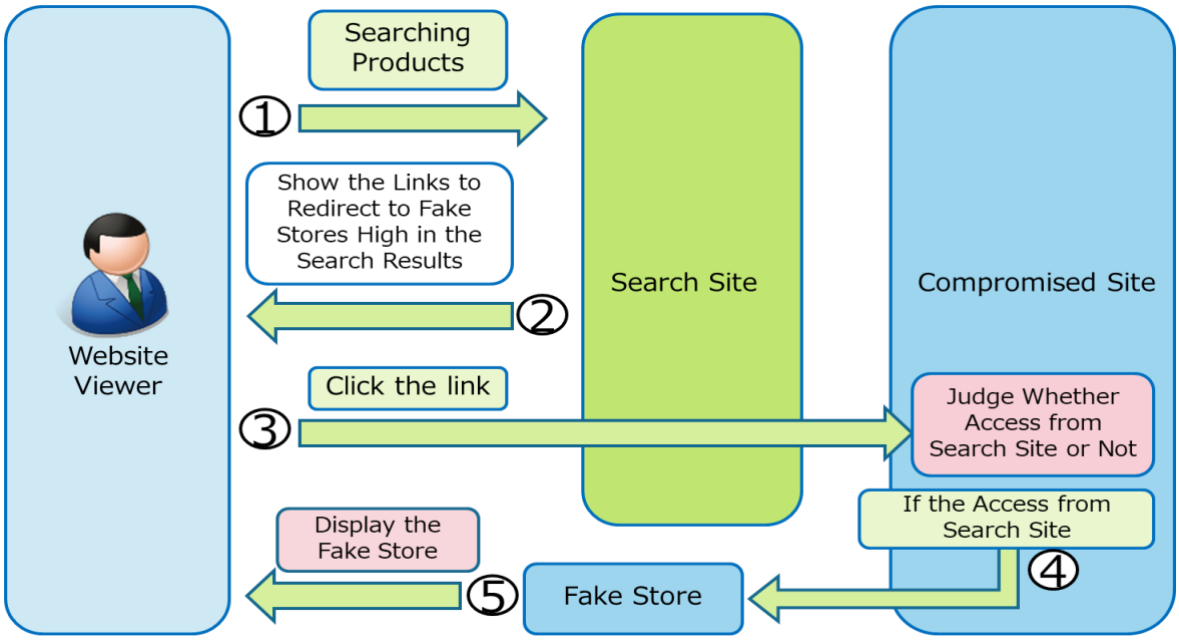

Figure 3: Redirecting users to a “Fake Store” through a compromised website

Criminal groups have compromised websites around the world to embed product information and some redirection code to induce users to their “Fake Stores”. JC3 even found foreign legitimate firm’s websites and foreign health clinic’s website were compromised for that purpose.

Needless to say, hacking into any website is illegal. There is no reasonable expectation that a legitimate online shopping website will redirect a user by committing a crime, so it is clear that

forwarding website traffic through compromised websites should be judged to be a “Fake Store” managed by criminal groups, even though they look like legitimate online shopping websites.

3.2.2 Type 2: Frequent changes of company profile

On “Fake Stores”, frequent changes of their company profile, including contact information, have been observed. It’s apparent that the criminal group’s intent is to avoid being identified among users as a “Fake Store”. For instance, some “Fake Stores” display different company profiles each time a user accesses them with a different IP address, in spite of no change of product information (See Figure 4).

There is no need for any legitimate shopping website to change their company profile with each user. It is clear that an online shopping website that has very frequent changes of its company profile to deceive users should be judged to be a “Fake Store” managed by criminal groups.

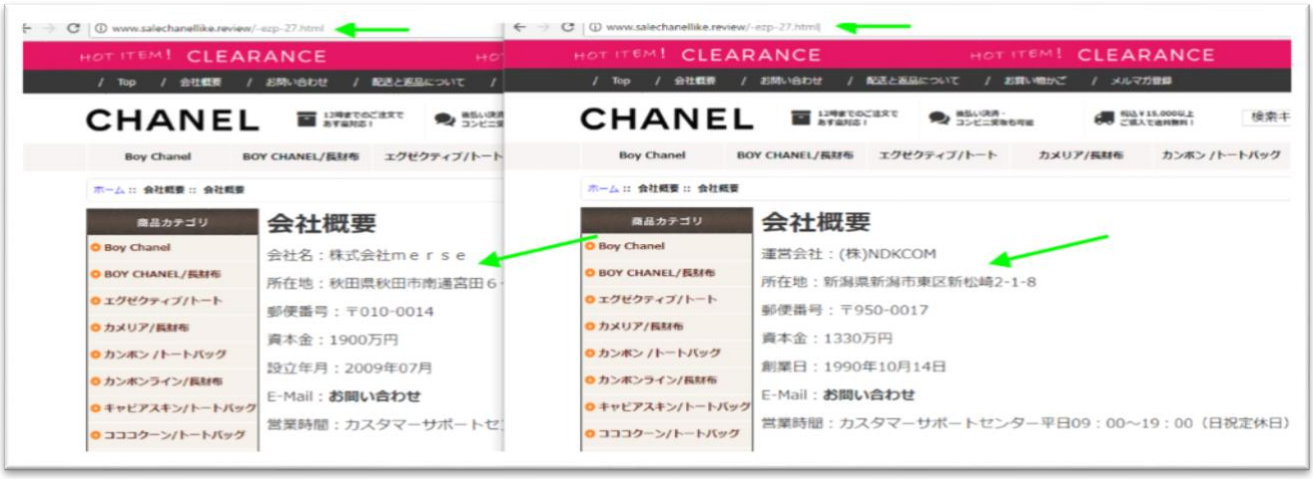

Figure 4. Viewing the same URL of a “Fake Store” using non-cached browsers on different IP addresses

3.2.3 Type 3: Lack of legitimate company profile

Because criminal groups don't have any legitimate company profile, most "Fake Stores" give users a non-existent company's name or pretend to be a legitimate company without their permission, also presenting factually inaccurate information such as their address or other contact information.

A legitimate company profile includes a business name, an address, and a phone number of a business operator licensed to operate in Japan. This profile is required to be displayed to the public by Act on Specified Commercial Transactions[4]. Therefore, an online shopping website that has non-existent or fake company profiles instead of legitimate company profiles should be judged to be a "Fake Store" managed by criminal groups[5].

[4] Refer to the 'Act on Specified Commercial Transactions Guide' (http://www.no-trouble.go.jp/foreignlanguage/) run by Consumer Affairs Agency, Government of Japan.

[5] The name and the address of the head office or principal place of business of each organization that has registered its indications by law in Japan are searchable on the 'Corporate Number Publication Site' run by National Tax Agency Japan. (http://www.houjin-bangou.nta.go.jp/)

4. Collecting information on “Fake Stores”

JC3 has been seeking to comprehensively identify and collect complete data regarding “Fake Stores” run by criminal groups, having similar characteristics. Although most of them are not yet recognized as fraudulent websites, they will soon victimize individuals.

4.1 Characteristics of “Fake Store” Criminal Groups

JC3 categorized the criminal groups, who have been operating “Fake Stores”, into six types based on their characteristics.

4.1.1 “Fake Store” Criminal Group A

The characteristic of the “Fake Store” criminal group A is as follows.

- Embedded code into a compromised website will redirect users to the “Fake Stores” via proxy websites (e.g. topvipsales.top or snacksshop.top): Type 1.
- The “Fake Stores” lack legitimate company profiles. Some of them pretend to be a legitimate company with factually inaccurate information: Type 3.
- The “Fake Stores” have been periodically changing the design and the content of the entire storefront.

4.1.2 “Fake Store” Criminal Group B

The characteristic of the “Fake Store” criminal group B is as follows.

- The “Fake Stores” frequently change their company profile each time an IP address of a user is changed: Type 2.
- Several specific email accounts (e.g. order@byselljp.com, 123@byselljp.com) are recycled for registration information of the domains used to host “Fake Stores”.

4.1.3 “Fake Store” Criminal Group C

The characteristic of the “Fake Store” criminal group C is as follows.

- The “Fake Stores” lack legitimate company profiles, having non-existent company names and factually inaccurate information: Type 3.
- The “Fake Stores” use the identical file name ‘会社概要-ezp-7.html’ for their company profile pages.

4.1.4 “Fake Store” Criminal Group D

The characteristic of the “Fake Store” criminal group D is as follows.

- Embedded code into a compromised website will redirect users to the Fake Stores: Type 1.

- The “Fake Stores” have non-existent or fake company profiles instead of legitimate company profiles: Type 3.
- The “Fake Stores” use the identical file name ‘/page/?id=11’ for their company profile pages.

4.1.5 “Fake Store” Criminal Group E

The characteristic of the “Fake Store” criminal group E is as follows.

- The “Fake Stores” lack legitimate company profiles, having non-existent company’s name and factually inaccurate information: Type 3.
- All the “Fake Stores” in this group have been periodically changing the contact email addresses at the same time
- Incomprehensible explanations are seen too many times about the payment. For instance, users can actually only choose credit card payment in spite of the description that users can choose both card payment and bank transfer.

4.1.6 “Fake Store” Criminal Group F

The characteristic of the “Fake Store” criminal group F is as follows.

- Embedded code into a compromised website will redirect users to the Fake Stores: Type 1.
- The “Fake Stores” have non-existent or fake company profiles instead of legitimate company profiles: Type 3.
- Several specific email accounts are recycled for contact information, even though the “Fake Stores” have different company profiles.
- The “Fake Stores” use the identical file name ‘/aboutus.html’ for their company profile pages.

4.2 “Fake Stores” Run by Each Criminal Group

Based on the characteristics of each “Fake Store” criminal group mentioned, JC3 has been worked to comprehensively identify and collect all of the “Fake Stores” that the criminal groups have made with similar modus operandi. At the end of 2017, JC3 identified the following volume of “Fake Stores” that were living and able to be used to victimize individuals at that time, even though most of them are not yet recognized as fraudulent websites.

Chart 1: Number of “Fake Stores” Run by Each Criminal Group (2017)

Group	Number of URL
A	7,817
B	5,483
C	197
D	2,841
E	2,497
F	999
Total	19,834

5. Mitigation of damage of “Fake Stores”

JC3 has been providing information of newly identified “Fake Store” websites to APWG and JC3’s member companies including security software providers and IT security vendors. In addition, JC3 has publicly warned internet users about the “Fake Stores” in order to mitigate the threat they represent to users.

5.1 Providing Information about “Fake Stores”

For mitigation of the damage caused by the “Fake Stores”, JC3 provided APWG and JC3’s member companies including security software providers and IT security vendors with the 19,834 URLs of the “Fake Stores” identified as mentioned in section 4.2 in order to display an alert on users’ PCs when they view them.

Nevertheless, the “Fake Stores” don’t meet the APWG’s criteria mentioned in section 2.1. So, some APWG member companies that seem not yet to recognize the threat of these “Fake Stores” don’t adopt the URLs JC3 provided APWG to use their alert system for users. In the near future, it is expected that APWG should adopt and promote a new threat definition of “Fake Store” as a harmful threat for users.

5.2 Warning against “Fake Stores”

In addition, JC3 has warned internet users about the threat and modus operandi of “Fake Stores” through the JC3 website and published a press release describing the countermeasures against the threat in cooperation with Japanese police for the purpose of alerting the public of the viciousness of “Fake Stores”.

5.2.1 Crackdown of Criminals Related to “Fake Stores”

Based on the JC3’s analysis, Japanese police conducted a nationwide crackdown targeting the account holders whose bank accounts were used for payments on “Fake Stores” and arrested 43 criminals. Moreover, police departments across Japan gave a security guidance about neutralizing them to the administrators of the 272 compromised Japanese websites that redirected users to “Fake Stores”.

5.2.2 Prevention Countermeasures

JC3 provided APWG and JC3’s member companies including security software providers and IT security vendors with 19,834 URLs of “Fake Stores” that JC3 identified.

5.2.3 Warning by JC3

The JC3's website[6] has published a caution about the characteristics of "Fake Stores", and the critical points described below, to protect individuals from becoming victims.

- Confirm that you are not automatically redirected to a "Fake Store" without realizing.
- Confirm that a shopping website you are viewing doesn't use an unfamiliar top level domain (TLD) like '.top' or '.xyz' or '.bid'.
- Confirm that the shopping website has a legitimate company profile including the name, the address, the contact information and the responsible person, not a non-existent or fake company profile.
- Confirm that the shopping website use an encrypted communication, meaning 'https', on its login page and its payment page.

[6] Refer to the JC3 website (https://www.jc3.or.jp/topics/malicious_site.html).

6. Conclusion

A “Fake Store” threat has been causing significant damage in Japan and is one of the more vicious website types being consistently operated by criminal groups. They’re designed for the sole purpose of stealing money and sensitive information, while posing as legitimate online shopping websites.

Given this situation, JC3 has been providing APWG with the URLs of “Fake Stores”, however, only some APWG member companies adopt the URLs to display an alert on users’ PCs, because the “Fake Stores” don’t meet the APWG’s core phishing website criteria.

Therefore, in the near future, it is expected that APWG should establish a new definition of “Fake Store” as a harmful threat for users. It is also expected that more APWG member companies leverage the URLs of “Fake Stores” that JC3 has been providing to APWG, in order to use in their alerting systems to protect users from the threat of “Fake Stores”.

We hope this white paper will help to minimize the threat of “Fake Stores” and reduce the number of victims that “Fake Store” websites compromise. We hope that APWG members will benefit from this research and work to protect other Internet users because these cyber criminals are not targeting a specific country or language[7].

[7] Refer to appendix (7.3 “Fake Stores” in English).

7. Appendix

7.1 Research Items of Malicious Websites

JC3 researched 7,000 malicious websites reported to Police from victims who have had money or credential information stolen about the items below;

- Registration information on WHOIS such us name, address, phone number, email address, registrar, date of registration and update
- IP address and domain information
- Content of websites including design, language, product information, company profiles, access analysis tool and payment method

7.2 Detail of Characteristics of "Fake Stores"

7.2.1 "Fake Stores" appearing high in search results

When a user searches a product for their purchase, some compromised websites appear high in the search results, since criminal groups have embedded code[8] into the compromised websites in order to redirect users to their "Fake Stores".

- Even some overseas legitimate website unrelated to any shopping sites were compromised to embed code.
- For some big frameworks, embedded code into one compromised website has hundreds of details of products and redirect scripts to hundreds of "Fake Stores" using servers where numerous data of products and URLs of "Fake Stores" are stored.
- "Fake Stores" themselves seem to avoid to register by web crawling bots.

7.2.2 Infrastructures used for "Fake Stores"

Infrastructures including IP address and domains used for "Fake Stores" are characterized by the following points.

- Common IP addresses and email accounts are used for many domains used for "Fake Stores".
- While criminal groups seem to get hundreds of domains at the same day, these domains are used for a month or a couple of weeks at shortest.
- Content of "Fake Stores" are apparently composed of stolen image data of products from legitimate shopping websites.

---

[8] You can see a sample of the code on Github (https://github.com/abshkd/malware/blob/master/shells/wp-darkshell/installer.php).

7.2.3 Unnatural expression on “Fake Stores”

Unnatural expressions are often seen on “Fake Stores”. The following sentences make native Japanese speakers feel weird.

<Sample 1>
http://www.machigakuji.pw/
安全のために秘密にする、E-MAIL 里告知する。

<Sample 2>
http://www.machigakuji.pw/faq.aspx
販売しているブランドは本物ですか、どうしてそんな安い？

当店の取扱い商品は、直接に工場より買付けをしていますので、100%新本物ですのでご安心ください。または、激安な単価で販売します。このごろ、お客様に多くのサービスが行っているので、商品はバーゲンセールをします。弊社の商品は高品質で、お客様が好きになったら、ぜひご注文ください。

<Sample 3>
・http://accessoriesonlinejp.bid/
全世界送料無料（画像）

7.3 “Fake Stores” in English

In 2018, JC3 newly found that some “Fake Store” criminal groups seemed to change or expand their targeted fields from Japan to abroad in order to steal credit card information.

- As of April 2018, a “Fake Store” in English was confirmed to be built with the domain (https://www.aiidao.online/) that the group D used for a “Fake Store” in Japanese in January 2018, and
- As of April 2018, a “Fake Store” in English was confirmed to be built with the domain (https://www.zdjitu.info/) that the group F used for a “Fake Store” in Japanese in December 2017.
- Specific email accounts (e.g. 247serviceonline@gmail.com, buycontactsonline@gmail.com) are used for contact email addresses on hundreds of “Fake Stores” in English.