



**National center of Incident readiness and
Strategy for Cybersecurity**

Findings and Expectations from cooperative works with ASEAN Member States

October 2, 2019



ASEAN • JAPAN

Cybersecurity Cooperation

1. Overview of AJ-CPM:
ASEAN-Japan Cybersecurity Policy Meeting
2. Introduction of an activity of AJ-CPM:
Voluntary Mutual Notification Program -
Government owned website defacement



AJ-CPM;













- A framework of Cybersecurity Authorities for promoting cybersecurity policy cooperation among ASEAN Member States and Japan.
 - NISC, Japan serves as secretariat of AJ-CPM.
- Established in 2009
- Acknowledged at "ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation" in 2013.

We believe that a secure cyberspace is one of the major drivers in innovation as well as being essential in promoting social and economic activities and strengthening ASEAN connectivity

The "Joint Ministerial Statement" of the Meeting
(13 Sep, 2013)

- Encourages to promote joint efforts in the areas of:
 1. Creating a secure business environment
 2. Building a secure information and communication network
 3. Enhancing capacity for cyber security

Member Agencies

		Member Agencies of AJ-CPM		Cooperative Agency
		Cybersecurity Authority	National CSIRT	
	Brunei	NSC	BruCERT	
	Cambodia	MPTC	CamCERT	
	Indonesia	BSSN	ID-SIRTII/CC	MCIT
	Japan	NISC	NISC, JPCERT/CC	MIC, METI, MOFA, JPCERT/CC, JICA, IPA, JC3
	Laos	MPT	LaoCERT	
	Malaysia	NACSA	NC4	MCMC
	Myanmar	MOTC, NCSC (of MOTC)	mmCERT	
	Philippines	DICT	NCERT	
	Singapore	CSA	SingCERT	MCI
	Thailand	MDES	ThaiCERT	ETDA
	Vietnam	AIS	VNCERT	
	ASEAN Secretariat			

- The AJ-CPM has endorsed to promote 8 CAs.
 - Yearly activity that all Member Agencies are participating.
 - Lead by “Lead Country”
 - Output should be reported to AJ-CPM.
- 1. Cyber Exercise (Lead by Japan)
 - Plan and conduct two types of cyber exercise
- 2. CIIP Workshop (Lead by Indonesia)
 - Plan and conduct a one day Workshop for policy makers to learn best practice of CIIP
- 3. Joint Awareness Raising (Lead by Brunei)
 - Share the practices and materials of awareness raising

4. Capacity Building (Lead by Thailand)
 - Share the information of the training courses for AMS
5. Voluntary Mutual Notification Program (Lead by Japan)
 - Voluntary notify threat information when one country find sign or incident in another country
6. Online Community for Policy Maker (Lead by Singapore)
 - Facilitate the web-based "Online Community" for sharing information include press release and reports
7. ASEAN-Japan Cybersecurity Reference
(Lead by ASEAN Secretariat)
 - Maintain the Reference
8. WG Steering (Lead by Japan)
 - Plan and review collaborative activities for next and following years

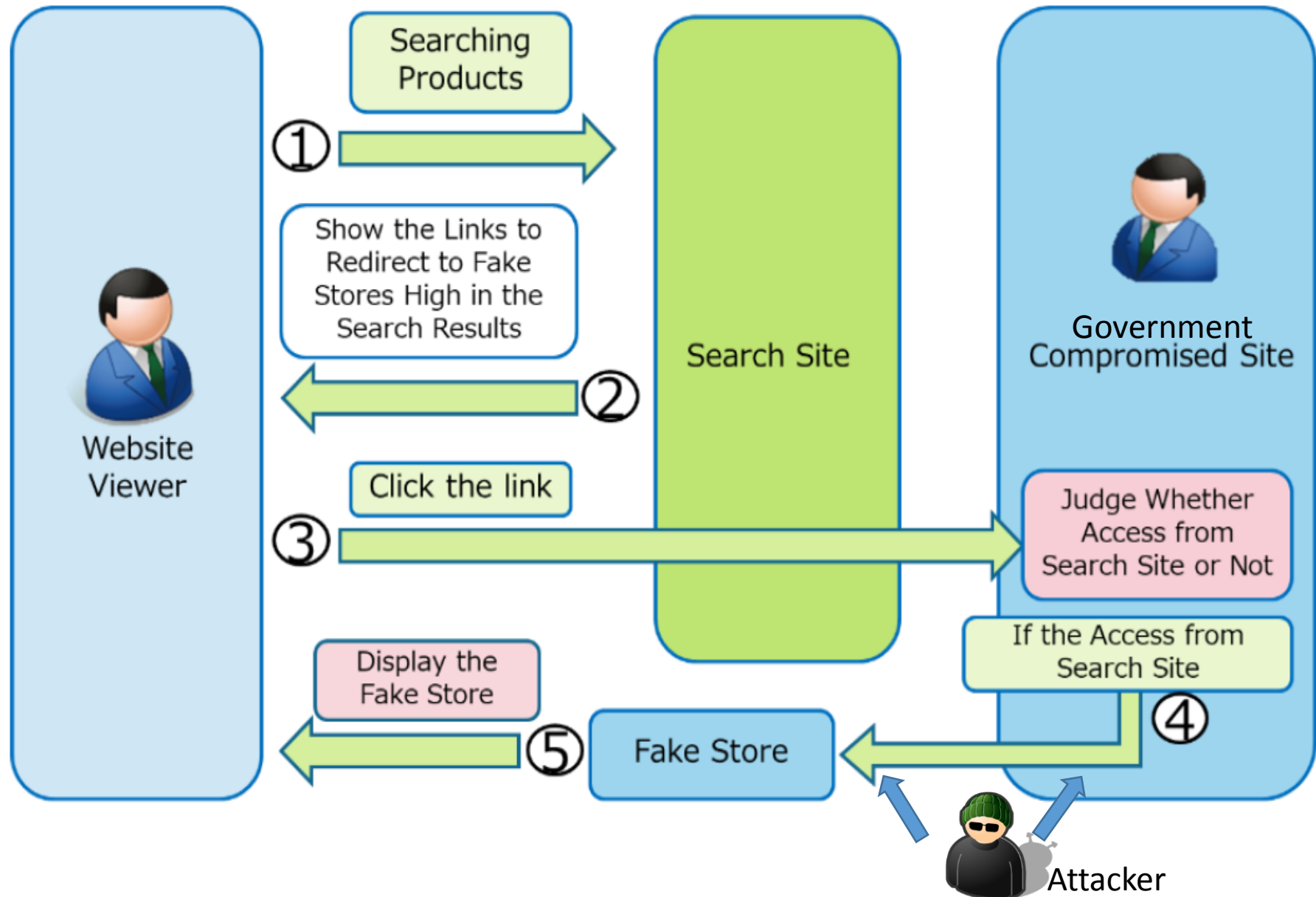
Voluntary Mutual Notification Program

Case AJ01:
Government owned website defacement



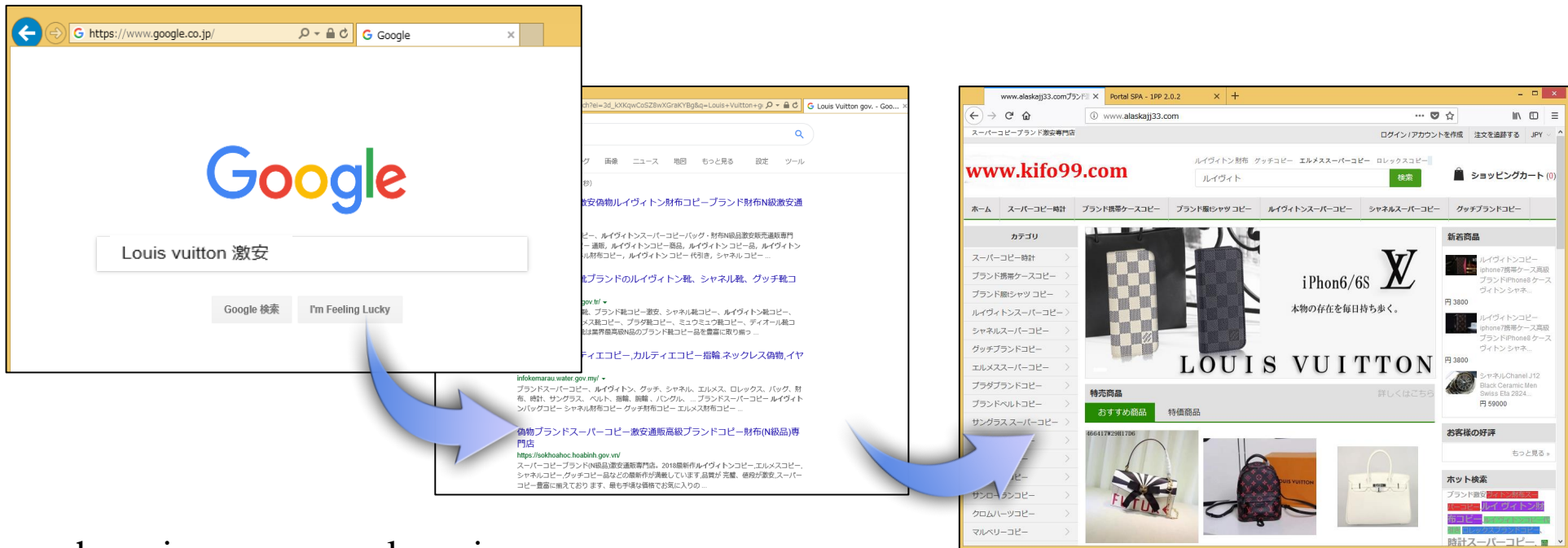
- Attackers embed redirect code in the government website for leading the web crawlers to a fake shopping site
 - A SEO (Search Engine Optimization) technique for attracting more people to the fake shopping site.
 - The site can earn high page rank of the search engine.
 - The embedded URL is not visible for the visitors of government website.

- The victim:
 - not only the customers of the fake shopping website
 - but also administrators of government website.



How to find? It's quite simple.

- The customer looking for the products at the search engine will be misled to the fake shopping site.



search engine: google.co.jp
language setting: Japanese
query: Luis Vuitton .gov

Example: search result

The screenshot shows a Google search interface with the query "Louis Vuitton gov." in the search bar. The results page displays four search results, each with a green callout bubble highlighting the domain and country. The first result is for "gov.pk (Pakistan)" with the URL "www.nlp.gov.pk/" and a description of a high-end counterfeit store. The second result is for "gov.tr (Turkey)" with the URL "www.smenetworking.gov.tr/" and a description of a high-quality counterfeit shoe store. The third result is for "gov.my (Malaysia)" with the URL "infokemarau.water.gov.my/" and a description of a brand super-copy store. The fourth result is for "gov.vn (Viet Nam)" with the URL "https://sokhoahoc.hoabinh.gov.vn/" and a description of a counterfeit brand super-copy store.

Google Louis Vuitton gov.

すべて ショッピング 画像 ニュース 地図 もっと見る 設定 ツール

約 6,130,000 件 (0.25 秒)

ブランドコピー激安 gov.pk (Pakistan) ブランド財布N級激安通
販 ...
www.nlp.gov.pk/ ▼
最高級ルイヴィトンコピー、ルイヴィトンスーパーコピーバッグ・財布N級品激安販売通販専門
店、ルイヴィトンコピー 通販、ルイヴィトンコピー商品、ルイヴィトンコピー品、ルイヴィトン
バッグコピー、シャネル財布コピー、ルイヴィトンコピー 代引き、シャネルコピー ...

スーパーコピー靴ブランドの gov.tr (Turkey) グッチ靴コ
ピー通販
www.smenetworking.gov.tr/ ▼
高品質スーパーコピー靴、ブランド靴コピー激安、シャネル靴コピー、ルイヴィトン靴コピー、
グッチ靴コピー、エルメス靴コピー、プラダ靴コピー、ミュウミュウ靴コピー、ディオール靴コ
ピー、スーパーコピー靴は業界最高級N品のブランド靴コピー品を豊富に取り揃っ ...

ラプリングカルティエコピー gov.my (Malaysia) 偽物、イヤ
リング ...
infokemarau.water.gov.my/ ▼
ブランドスーパーコピー、ルイヴィトン、グッチ、シャネル、エルメス、ロレックス、バッグ、財
布、時計、サングラス、ベルト、指輪、腕輪、バンダナ、 ... ブランドスーパーコピー ルイヴィト
ンバッグコピー シャネル財布コピー グッチ財布コピー エルメス財布コピー ...

偽物ブランドスーパーコピー激安 gov.vn (Viet Nam) 偽品)専
門店
<https://sokhoahoc.hoabinh.gov.vn/>
スーパーコピーブランド(N級品)激安通販専門店。2018最新作ルイヴィトンコピー、エルメスコピー、
シャネルコピー、グッチコピー品などの最新作が満載しています。品質が 完璧、値段が激安、スーパー
コピー豊富に揃えており ます、最も手頃な価格でお気に入りの ...

Example: Compromised website and embedded code



embedded code

```
1
2 <script>
3   var s=document.referrer;
4   if(s.indexOf("google.co.jp")>0||s.indexOf("google.com")>0||s.indexOf("yahoo.co.jp")>0)
5   {
6     self.location="http://www.██████████.ducks/p4/3/242111/";
7   }
8 </script>
9
10
11
12
13 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
14 <html xmlns="http://www.w3.org/1999/xhtml">
15   <head>
16     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
17     <title>Portal SPA - v3.1.2</title>
18   </head>
19
20   <script>
21     if (window != top) top.location.href = location.href;
22   </script>
23
24
25   <script src="resources/js/ext-core.js"></script>
26   <script src="resources/js/portal.js"></script>
27
```

source html file of the government official website

Example: Fake Shopping Site

The screenshot shows a web browser window displaying a fake shopping site. The address bar shows the URL **www.kifo99.com**. The site's header includes a search bar with the text "レイヴィト" and a navigation menu with categories like "ホーム", "スーパーコピー時計", "ブランド携帯ケースコピー", "ブランド服tシャツ コピー", "ルイヴィトンスーパーコピー", and "シャネルス".

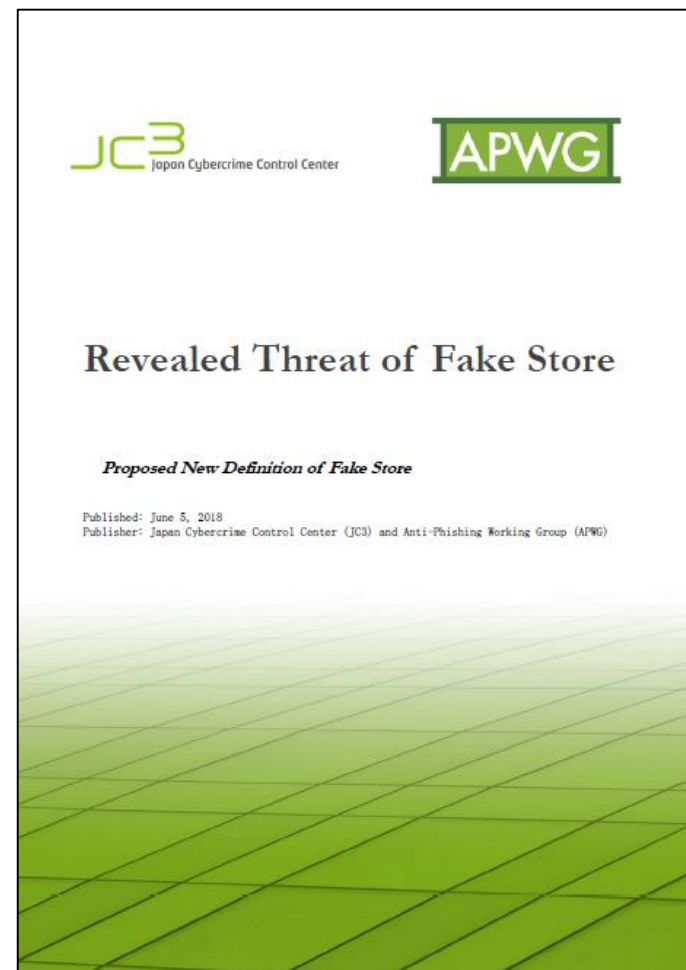
A dropdown menu for currency selection is open, showing options: US Dollar, Euro, GB Pound, Canadian Dollar, Australian Dollar, CNY, Japanese Yen, New Zealand Dollar, Danish Krona, and Norwegian Krone. The "US Dollar" option is highlighted.

To the right, a "LANGUAGES" section lists various languages with corresponding flags: Deutsch, French, Italiano, Spanish, Portuguese, Chinese, Norwegian, and Japanese.

The main content area features a large advertisement for "LOUIS VUITTON" with the text "iPhone6/6S" and "本物の存在を毎日持ち歩く。". Below this, there are sections for "特売商品" (Special Sale Items) and "おすすめ商品" (Recommended Items), each displaying images of various handbags and accessories.

A red speech bubble points to the language selection list with the text: "The targeted customer is not only Japanese".

- Please refer to the report for more detail of AJ01 by JC3 and APWG
 - Japan Cybercrime Control Center
 - Anti Phishing Working Group, US



https://www.jc3.or.jp/about/pdf/JC3_APWG_Revealed_Threat_of_Fake_Store.pdf

- AJ-CPM has been aware of the case AJ01 and decided to take voluntary coordinated action against it, since 2018.
- AJ-CPM focus on the compromised government website
 - Cybersecurity of the government owned website is the duty of the Cybersecurity Authority and National CSIRT.
- AJ-CPM don't focus on the fake shopping site
 - The law enforcement community is already working for it.
 - AJ-CPM will collaborate with them if needed.

- Some government websites have some vulnerability and the attacker abuse it.
 - Some of the AMS need help for better awareness and taking proper security measures.
 - The attacker may do some more serious things on the website.

- What we should do first is capacity building for AMS officials.
 - Japan, as a secretariat of the AJ-CPM, is coordinating with Cybersecurity Authorities of AMS to develop capacity building course.
 - Case AJ01 would be used as a good case study for making this capacity building project in a more practical manner.

- Short term: individual cybersecurity capability
 - Develop training course for National CSIRTs
 - ✓ create education materials specialized to the case AJ01
 - Improve domestic information sharing network
 - ✓ share the knowledge with local office and get better awareness

- Long term: collective cybersecurity capability
 - Enhance international information sharing
 - ✓ create the culture of the cybersecurity
 - ✓ foster trust among AMS and international partners

- Outcome: improve cyber hygiene in the region
 - Stimulate discussion for ASEAN Regional CERT

Develop training course for National CSIRTs	Develop learning materials	JICA has started to develop the materials for webserver security. The materials would be shared with AMS.
Improve domestic information sharing network	Develop a reference model for information sharing	AJ-CPM has developed the scenario for "Cyber Exercise" focusing on the domestic/international information sharing. This scenario can be used as a reference model to find gaps on existing network of each AMS.
	Raise awareness of the case AJ01	JC3 gives a lecture for AJ-CPM
Enhance international information sharing	Designate POC for international coordination	AJ-CPM maintain International POC list of AMS and Japan

- Your knowledge and experience would be valuable for AJ-CPM to tackle with the case AJ01.
 - situational awareness of the case AJ01 and similar case
 - technical skills / check lists for web server protection
 - good practices / policy framework for web server protection

- It is welcomed if you have any idea of practical partnership with AJ-CPM.
 - technical information sharing (IoC, TTP, technical reports, ...)
 - capacity building (seminar, workshop, technical training, ...)

- Contact:
 - International Strategy Group, NISC, Japan
 - email: poc@nisc.go.jp

ご清聴ありがとうございました

Thank you for your attention