



Phishing in the Oasis:

Investigating the 2 year real estate data harvesting campaign targeting the Middle East

Author: Anirudh Batra



INDUSTRY:
REAL ESTATE

REGION:
MIDDLE EAST

White papers and reports can be downloaded from the CloudSEK website by visiting <https://cloudsek.com/whitepapers-reports> or by mailing to info@cloudsek.com.

At CloudSEK we have been monitoring the increment of data harvesting scams occurring in the Middle East market. One of the most affected markets is real estate due to increase of interest from foreign investors/oligarchs due to the ever changing geopolitical situation of the world.

Threat Actor groups understand this fact and love to capitalize on that. What we have been monitoring is the complete cycle of trade that has happened around illegal trade of data of leads/PII information even sorted nationality wise of people who are interested in buying properties in the Middle East.

This is not the first time a scam has erupted in the Middle East specially in prime Real Estate markets like the UAE, Qatar, Saudi Arabia etc. The sheer scale at which this scam has been operating is what makes it different from the earlier campaigns that have occurred in the middle east.

This whitepaper aims to uncover a trend in the market and make people aware, to understand the scale of this campaign and its rampant increase refer to the following numbers:

- We analyzed close to **6100 suspicious domains** created in the last 5-6 years
- We shortlisted about **~3500 domains** most of which were registered in the last 2 years namely from 2021-2023
- These domains were shortlisted based on a number of factors some of them are Domain name similarity to popular properties in the Middle East, Registrant Email, JARM hash, similar templates being used as well as phone numbers etc.

Please Note: This is just the tip of the Iceberg, these domains were found based on a wordlist of only 120 entries. During the process we found that Threat Actors have targeted properties which are yet to be completed, as that gives them more leg room to conduct a scam.

In this whitepaper we will try to analyze the trend, templates used, infrastructure and close it with understanding where this data is being sold and how you can save yourself from falling for this scam.

Trends and Timeline

This campaign was flagged by our contextual AI driven Digital Risk protection platform [XVigil](#) earlier this year because of the sheer number of domains being registered targeting two of the most premium upcoming properties in Dubai. When we dug deeper into the domains we realized the scale of the campaign. The below trendline demonstrates the timeline of ~3500 scam domains which have been registered in the last 2 years.

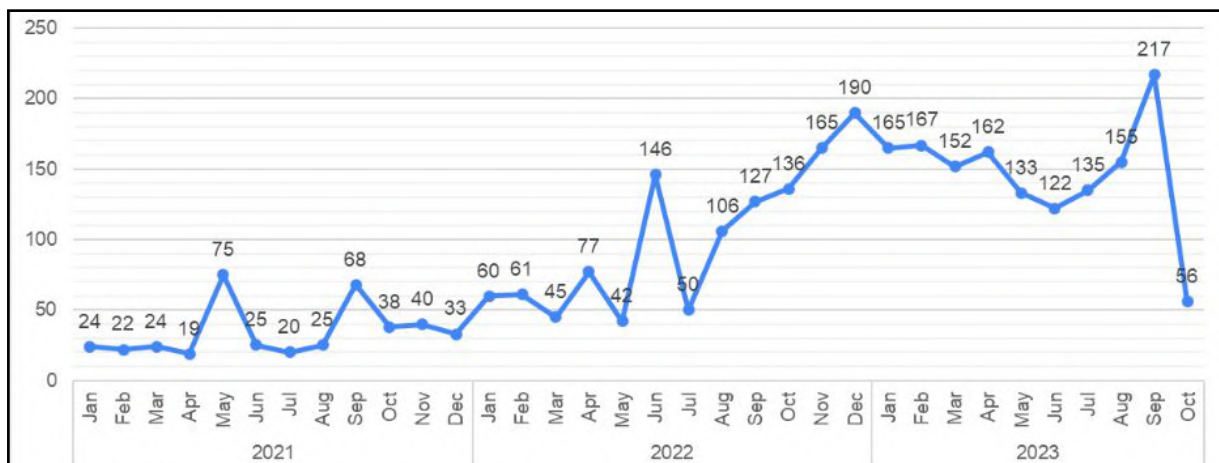


Figure1: Shows the trendline and number of domains being registered every month for the last 2 years

From the above trend we can see that the monthly average scam domain creation changed drastically in this year, there was a huge spike last month and October,2023 is still going strong.

These domains were registered on a number of different hosting providers. The top 5 most used are as follows:

1. GoDaddy
2. REG-RU
3. Namecheap
4. RU-CENTER-RU
5. CSC Corporate domains

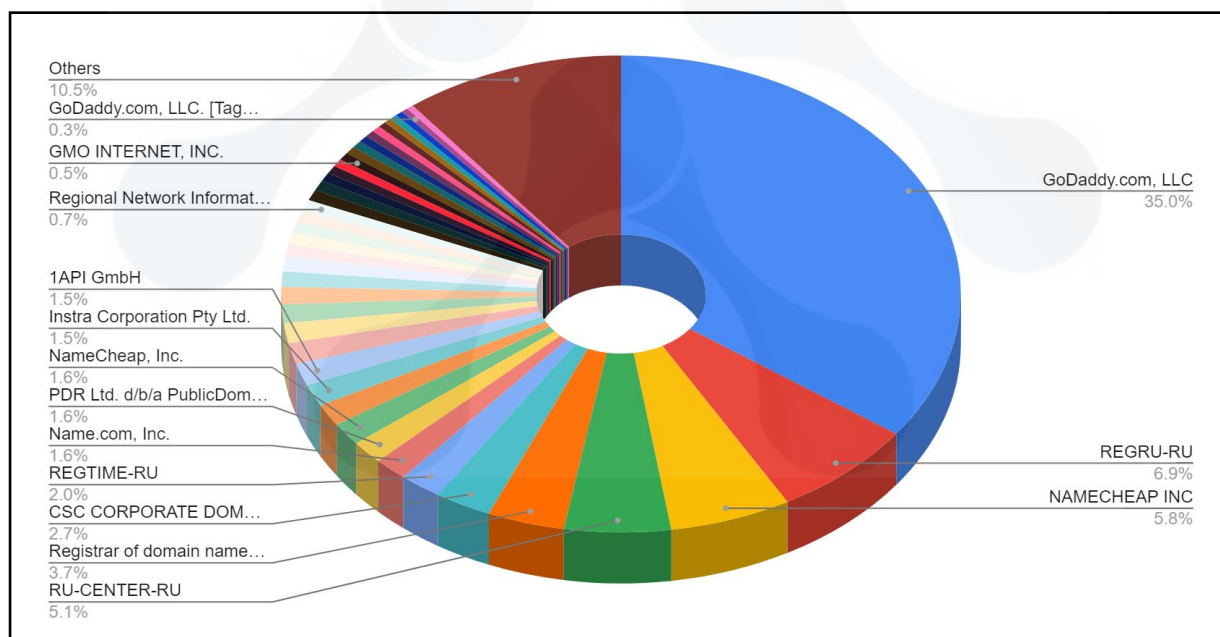


Figure 2: Pie chart showcasing the distribution of Registrars being used in the campaign

We see this trend due to multiple reasons:

1. Ease of registering a domain
2. Price of registering a domain
3. Payment options in cryptocurrency
4. Privacy options available while registering these domains

We can also see that out of the top 5 most used registrars 2 of them provide “.ru” TLD domains, which is a threat actor favorite for privacy and lack of regulation for abuse reports etc. but in this case there is one added advantage of increased trust among one of the most targeted nationalities in this scam that i.e Russian. Due to the ongoing conflict in the region we see a steep interest from Russian oligarchs to invest money in the UAE and Real Estate becomes a prime investment.

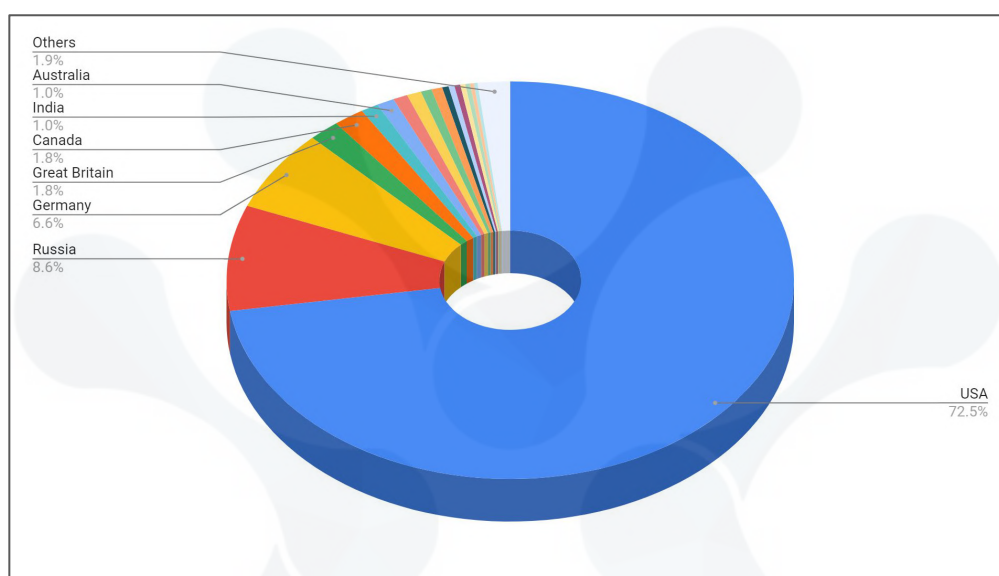


Figure 3: Pie chart showing the distribution of the countries associated with the A records of the scam domains

Figure 3 is a pie chart showing the infrastructure trend for the scam, these represent the country from where the IP addresses originate which are taken from the A records of the domains involved in this scam.


The most 5 most commonly found are:

1. USA
2. Russia
3. Germany
4. Great Britain
5. Canada

Here India and Australia are a very close 6th in the list

Some of the interesting observations made from the IP addresses found from this campaign are:

- There are only **~1330 unique IP addresses** in the scam hosting more than 6000+ suspicious domains, hence logically we have some groups operating multiple domains on a single IP which is a common practice
- The following IPs were used abnormally high times and have known to be operated by cyber criminals:

IP Address	Number of Domains mapped	Remarks
165.160.15.20	427	This IP has been marked malicious by VT and has previous history of being used for phishing, from the number of relations with malicious files this IP probably is used as a sinkhole(with low confidence)
165.160.13.20	436	This IP has been marked malicious by VT and has previous history of being used for phishing, from the number of relations with malicious files this IP probably is used as a sinkhole(with low confidence)
34.102.136.180	720	<p>This IP has been marked malicious by VT and has previous history of being used for phishing, from the number of relations with malicious files this IP probably is used as a sinkhole(with low confidence)</p> <p style="text-align: center;"><i>An interesting comment about the IP on Virustotal.</i></p> <div style="border: 1px dashed black; padding: 5px;"> <p> Blueightspecial 3 months ago</p> <p>This is also the ip for 3g3dprints.com. I know for a fact that this guy is a hacker. He lived next to me. He has been actively hacking my entire life and job for over 3 years non stop. He is very advanced and no one can help me get him stopped because it is over their head because what he does is very advanced and no one knows how to help me stop him because it is so beyond what anyone has ever heard of. I know for sure I am not the only person he is hacking. He is also a bitcoin miner so I have a feeling he is using my network to mine bitcoins and he is making me look like a hacker because he takes over my networks to hack and scam people. Help me get this cyber criminal stopped!!</p> </div>
64.190.62.22	73	This IP has been marked malicious by VT and has previous history of being used for phishing, from the number of relations with malicious files this IP probably is used as a sinkhole(with low confidence)

- We see a trend that on an average these IPs have had a history of communicating with more than 1.5k malicious binaries which led us to believe these are also being used as Sinkhole IPs[low confidence]
- We also thought it would be interesting to see the trend and analysis of ASNs used in this campaign and the following ASNs were the most used:
 1. AS13335
 2. AS22612
 3. AS16509
 4. AS46606
 5. AS47583

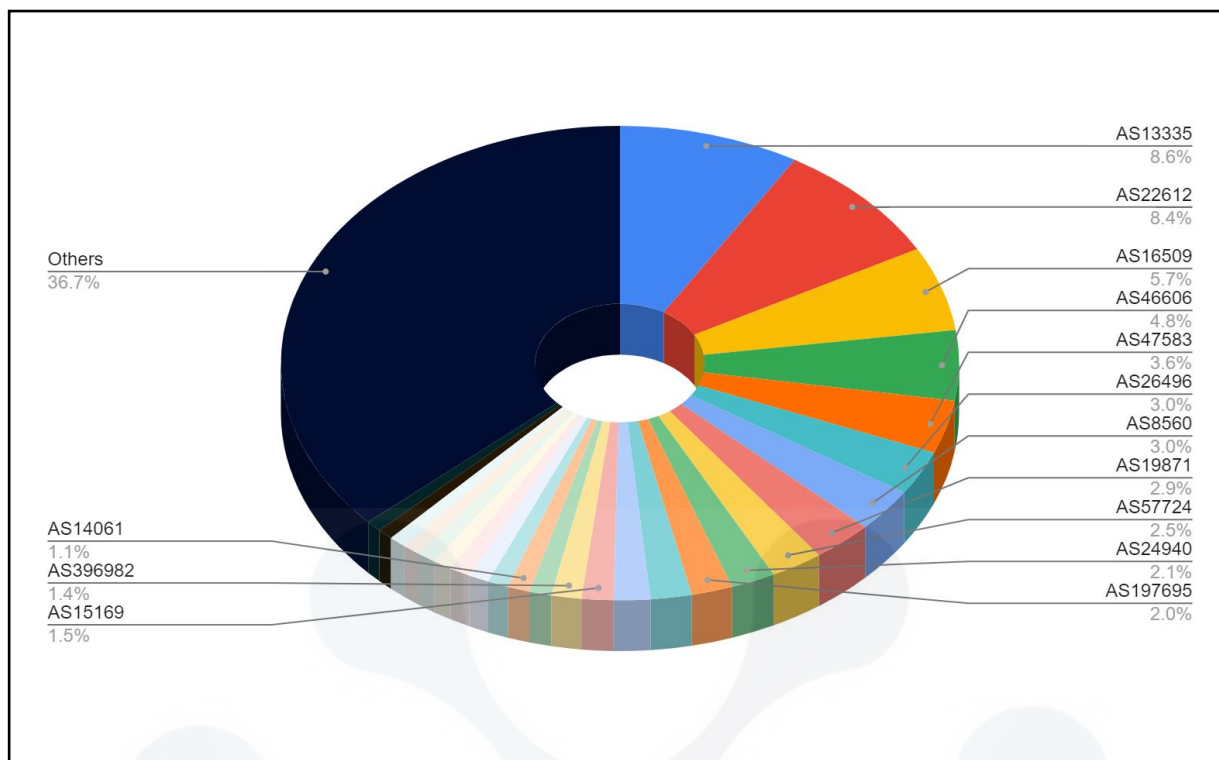
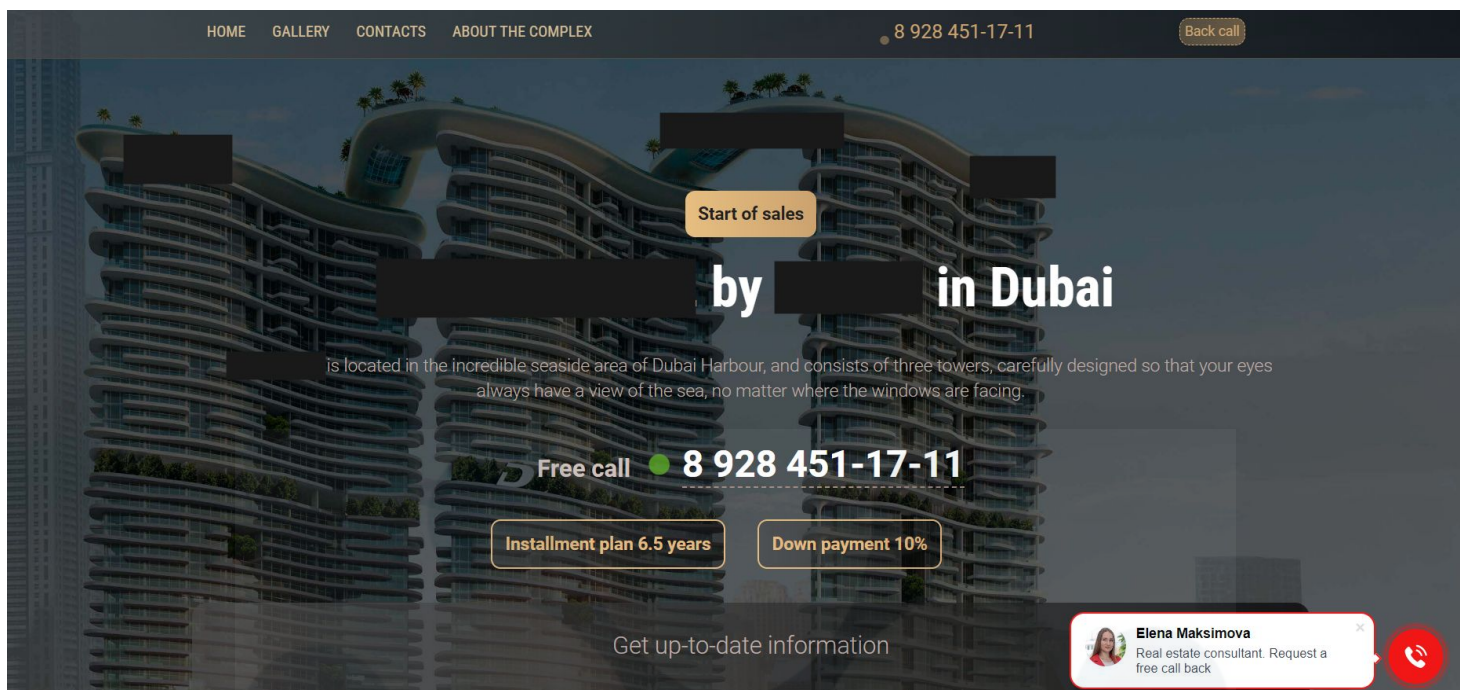


Figure 4: Pie chart showing the percentage analysis of malicious IPs originating from which ASN

Interesting Emails related to the Domains

Email	Remarks
wgviagens.hostgator@gmail.com	There are 1.5k+ domains registered with this email and most of which are fake/scam pages related to property or real estate
uk.dubai81@gmail.com	Only 5 domains registered on this email but all of them are pages involved in this Middle East campaign
makanecef@gmail.com	There are 17k+ domains registered using this email
tarkdomain@gmail.com	Only 12 domains registered on this email but all of them are pages involved in this Middle East campaign
mydomains99552@gmail.com	There are ~2.3k domains registered using this email. The domains are all real estate related scams and include properties not just from Middle East but India as well
pyslar-sergey@yandex.ru	Only 12 domains registered on this email but most of them are pages involved in this Middle East campaign
alez90@yandex.ru	Only 20 domains registered on this email but most of them are pages involved in this Middle East campaign



Screenshot 1: shows the template which is most commonly used by Threat Actors associated with this scam

1. The template has the same phone number - "**8 928 451-17-11**". If we use a simple google dork we get **200 results** of this number being used in this same template and involved in the real estate scam
2. The template uses Joomla as CMS, all of the domains use **Joomla v3.10.***
3. The domains are all **".ru"** TLDs
4. The domains have directory listing enabled and all the directories are mentioned in the robots.txt file.
5. The domains have an **/administrator** REST endpoint which is only protected by password to access backend systems.
6. The threat actors are using empire-crm.com to load all the functionalities
7. The template has been copied from this original website: [https://letniy-sochi\[.\]ru](https://letniy-sochi[.]ru), this can be confirmed from all the robots.txt files as it mentions the source to be the above mentioned URL
8. **RSfirewall** is being used which is a security extension offered by Joomla

```

Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/

Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /logs/

Disallow: /tmp/
Disallow: /component/
Disallow: /*mailto*
Disallow: /*start*
Disallow: /*print*
Disallow: /*feed*
Disallow: /*cart
Disallow: /*option=com*
Disallow: /*search*
Disallow: /*users*
Disallow: /*=rss*
Disallow: /*=atom*
Disallow: /edit?
Disallow: /virtuemart
Disallow: /index.php?option=com_content
Disallow: /*created_on?manage=*
Disallow: /*?manage*
Disallow: /*results*
Disallow: /dirasc?manage=*
Disallow: /dirDesc?manage=*
Disallow: /*created_on*
Host: https://letniy-sochi.ru/
    
```

Screenshot 2: shows one sample robots.txt file which also mentions the host

- 9. We have also noticed that these domains also contain images/documents related to other scam domains with the same template on the server

Domain name targeting one property

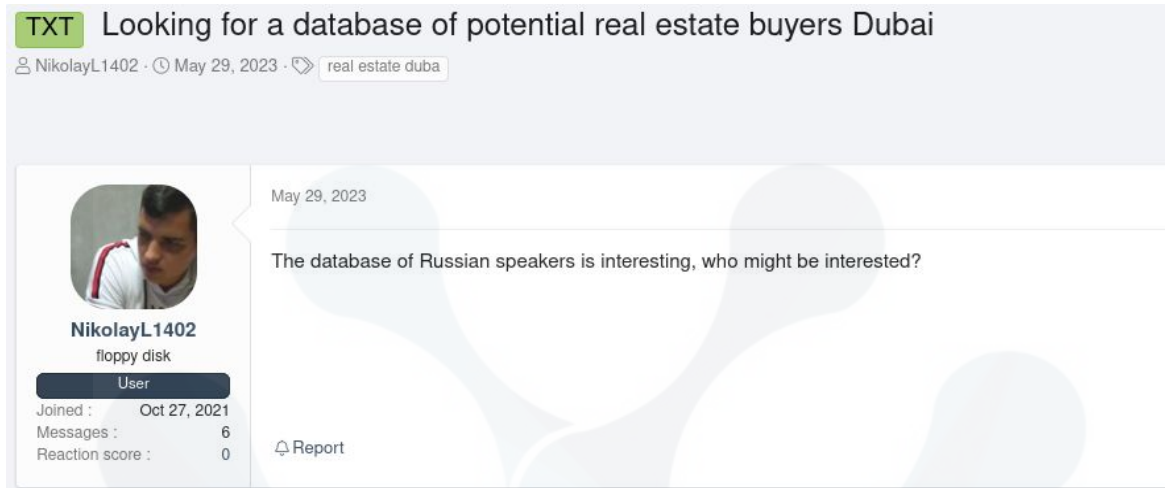
Index of /images/4

Name	Last modified	Size	Description
Parent Directory			
[redacted].mp4	2023-05-11 20:53	6.6M	Documents regarding a different property
[redacted]_ENG_16x9_WA.mp4	2023-05-13 13:52	3.1M	
[redacted](1)_compressed.pdf	2023-05-13 14:49	11M	
[redacted].page-0001_1.jpeg	2023-05-09 18:31	49K	
ame1_1.png	2023-05-09 16:58	925	

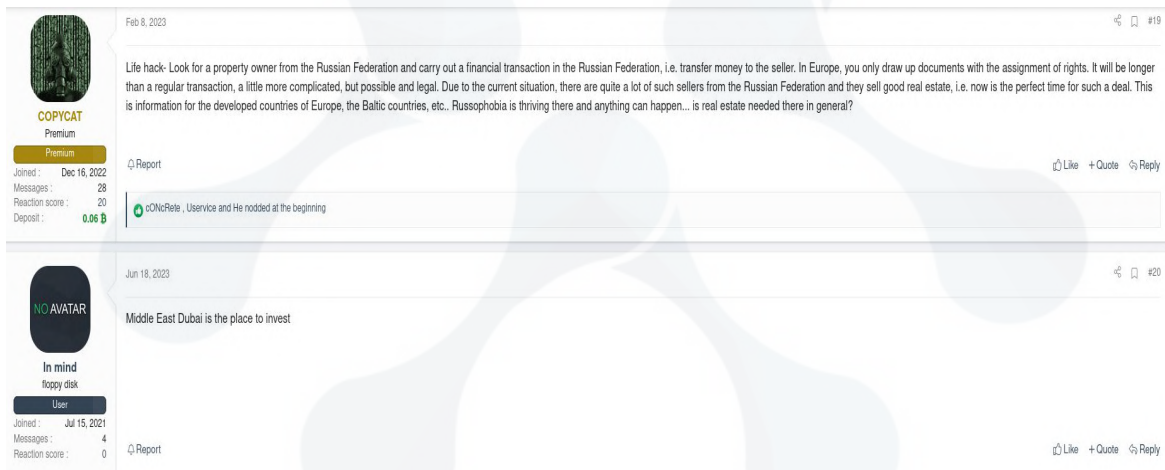
Documents regarding a different property

Screenshot 3: shows that the Threat Actors behind this campaign might be same or are at least using same TTPs

To run any campaign for a prolonged period of time there has to be demand for the data being sold, in this case we have seen the demand slowly growing and Threat Actors talking about the real estate market in Dubai. We also found a thread on a Russian Based forum regarding a Russian database of people interested in buying properties in Dubai. This completes the full circle.



Screenshot: shows specifically an interest in data of Russian nationals



Screenshot of a russian forum mentioning Dubai as a great place to invest in real estate

There are threat actors supporting investment in the Middle east real estate market as a way to launder money.

HUMAN INTELLIGENCE (SUPPLY OF DATA)

Our sources wanted to confirm the claim of Threat Actors claiming to share data. Our sources were able to obtain that data, one of the sources received a sample data in the format of an excel file containing 9MB worth data. The data had property wise and nationality wise segregation and we could infer that the data harvesting campaign has been in operation for at least 2 years. The threat actor had quoted a price of 1,000 USD for complete data.

A	B	C	D	E	F	G	H	I	J
Date	Master Project	Building	Size	Unit	Procedure	Name	Nationality		
4/10/2023			166.65	1203	Seller	ELTONLU	Canada		
4/10/2023			166.65	1203	Buyer	COMMERCIAL BANK OF DUBAI (PSC)			
4/10/2023			166.65	1203	Seller	PIA YUEN	Denmark		
4/10/2023			166.65	1203	Seller	WALEED ASG	Pakistan		
4/10/2023			166.65	1203	Buyer	ELTONLU	Canada		
3/31/2022			169.64	1204	Seller	SCOTT WILLI	New Zealand		
3/31/2022			169.64	1204	Seller	MARION LEI	New Zealand		
3/31/2022			169.64	1204	Buyer	HARRIS MIC	Canada		
6/21/2018			155.68	1302	Seller	ABDULRAHM	United Arab Emirates		
6/21/2018			155.68	1302	Buyer	NOOR BANK P. J.S.C			
7/25/2022			166.65	1303	Seller	VAHID ABBAS	Iran		
7/25/2022			166.65	1303	Buyer	ALI MOHAM	Iran		
3/24/2021			166.65	1303	Seller	SWAFIYA SAL	Kenya		
3/24/2021			166.65	1303	Buyer	VAHID ABBAS	Iran		
3/24/2021			330.89	1501	Seller	MONICA EFF	Panama		
3/24/2021			330.89	1501	Seller	GERARDO LU	United States of America		
3/24/2021			330.89	1501	Buyer	PEDER JUUL	Denmark		
4/16/2019			330.89	1501	Seller	GULF SHORES INC			
4/16/2019			330.89	1501	Buyer	GERARDO LU	United States of America		
4/16/2019			330.89	1501	Seller	MONICA EFF	Panama		
4/16/2019			330.89	1501	Seller	GERARDO LU	United States of America		
4/16/2019			330.89	1501	Buyer	NATIONAL BANK OF RAS AL- KHAIMAH (P.S.C)			
4/14/2022			256.83	1701	Seller	ALAWI SHUK	United Arab Emirates		
4/14/2022			256.83	1701	Seller	DARREN PUR	United Kingdom		
4/14/2022			256.83	1701	Buyer	John Leslie G	United Kingdom		
3/11/2018			256.83	1701	Seller	ALAWI SHUK	United Arab Emirates		
3/11/2018			256.83	1701	Buyer	MASHREQ BANK PSC			
9/6/2018			253.09	1702	Seller	FIKRI SONER	Turkey		
9/6/2018			253.09	1702	Seller	CEREN GOKC	Turkey		
9/6/2018			253.09	1702	Buyer	EMIRATES NBD BANK (P.J.S.C)			
12/28/2021			213.57	G01	Seller	KHADIJEH RE	Iran		
12/28/2021			213.57	G01	Seller	REZA KAZEM	Iran		
12/28/2021			213.57	G01	Buyer	AKBAR REZA	Iran		
3/8/2023			488.9	P01	Seller	AKBAR REZA	Iran		
3/8/2023			488.9	P01	Buyer	DUBAI ISLAMIC BANK (PUBLIC JOINT STOCK COMPANY)			
3/3/2023			488.9	P01	Seller	AKBAR REZA	Iran		
3/3/2023			488.9	P01	Seller	KHADIJEH RE	Iran		
3/3/2023			488.9	P01	Seller	REZA KAZEM	Iran		
3/3/2023			488.9	P01	Buyer	DUBAI ISLAMIC BANK (PUBLIC JOINT STOCK COMPANY)			
6/21/2023			65.96	101	Seller	SPL PC 15 Holding Limited			
6/21/2023			65.96	101	Buyer	SPL PC 15 HOLDING LIMITED			
11/25/2021			65.96	101	Seller	AJMAL SAIFI	Canada		

Screenshot of the sample shared by the Threat Actor

The Document shared by the threat actor also reveals some extra information in the metadata of the document, a simple exiftool command revealed the following information:

```
ExifTool Version Number      : 12.67
Directory                    : .
File Size                    : 9.5 MB
File Permissions             : -rwxrwx---
File Type                    : XLSX
File Type Extension         : xlsx
MIME Type                    : application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Zip Required Version        : 20
Zip Bit Flag                 : 0x0006
Zip Compression              : Deflated
Zip CRC                      : 0x8381b2c3
Zip Compressed Size         : 409
Zip Uncompressed Size       : 1833
Zip File Name                : [Content_Types].xml
Application                  : Microsoft Macintosh Excel
Doc Security                 : None
Scale Crop                   : No
Heading Pairs                : Worksheets, 3
Company                      :
Links Up To Date             : No
Shared Doc                   : No
Hyperlinks Changed          : No
App Version                  : 16.0300
Creator                      :
Last Modified By             :
Create Date                  : 2023:07:27 05:12:42Z
Modify Date                  : 2023:08:29 08:12:57Z
```

Screenshot: of metadata of the sample excel file shared by the threat actor with our source

Impact & Mitigation

It is important that we understand the impact this campaign can have on the region economically and otherwise.

- This scam provides a gateway for Threat Actors to lure people genuinely interested in the Real Estate and then scam them.
- From the above proofs we can be sure that this is a data harvesting campaign and that the data is available in enormous numbers. We can infer this from the size of the file shared by the Threat Actor just as a sample and that should be alarming.
- This reduces the brand reputation of the well established organizations in the region, this decrement in trust from the victims can impact them economically

We at CloudSEK have been actively reporting these incidents to the concerned organizations and we have initiated more than 150 takedowns helping the affected organizations and our clients.

There are some proactive methods that can be used to monitor and mitigate these threats:

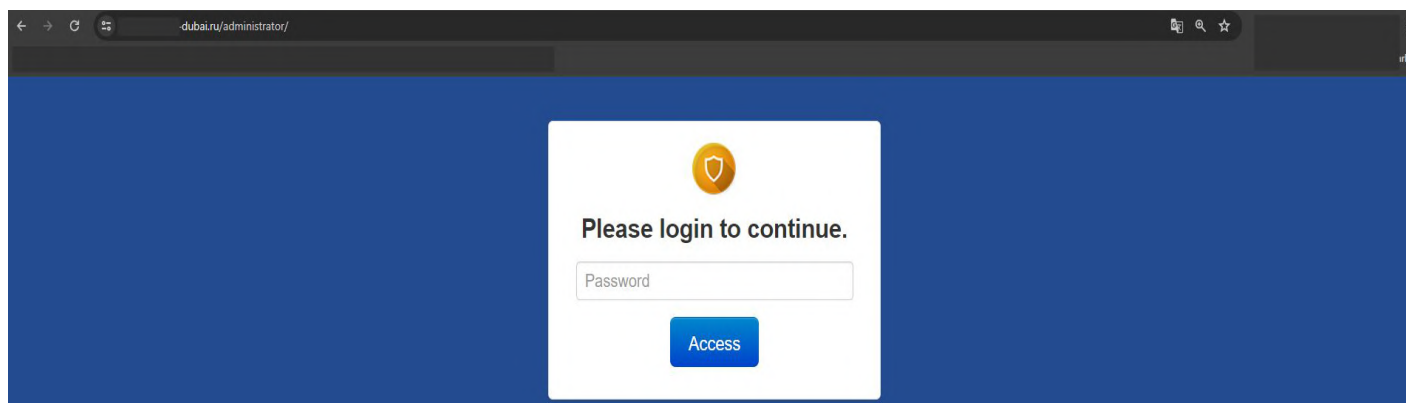
- Monitor newly created domains

- Invest in better SEO techniques so that the scam domains do not pop up above the original domains
- These domains should also be blacklisted from sending any email to an internal employee as this can be a double edged sword and can be used to target employees as well.

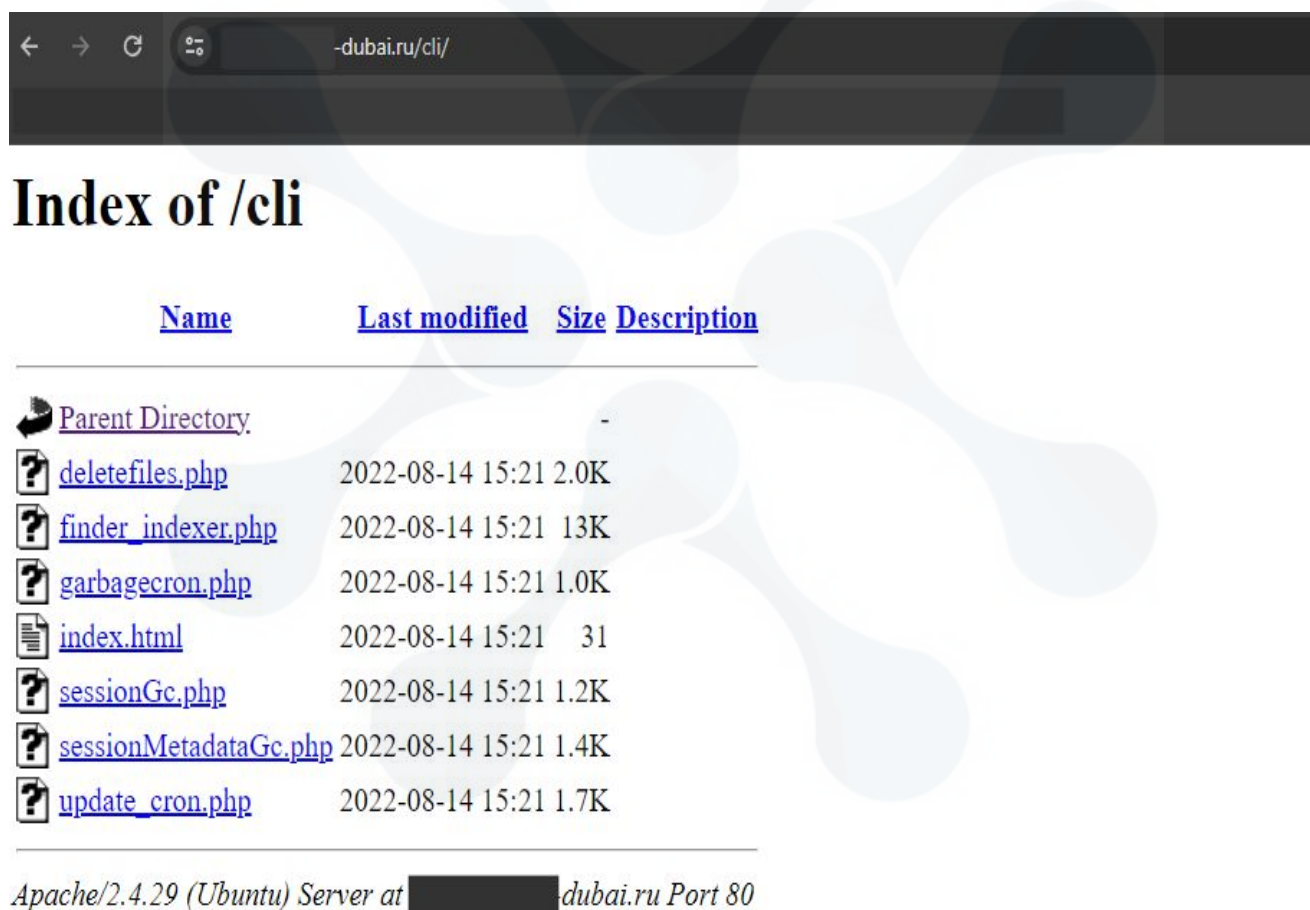
Appendix

All Emails found in the whois data of suspicious domains:

7086netflix@gmail.com a81287179@gmail.com acbudnjo@gmail.com adyjonathan22@gmail.com ahmedisit86@gmail.com akheelinfo@gmail.com a.nepomniashiy@gmail.com boriskinba@gmail.com bpd.domains@gmail.com ceooneplace@gmail.com christiantrucco@gmail.com creativedreams247@gmail.com elyassbouni@gmail.com finance.oleg@gmail.com fishemia@gmail.com greenacresindubai@gmail.com grgrgr1288@gmail.com info.serdcegoroda@gmail.com jawadhcheema@gmail.com Joshua37920@gmail.com luolanherosms@gmail.com makanecf@gmail.com marketing.toplevel.dubai@gmail.com matantsevarthem85@gmail.com meriieemjadi@gmail.com mishka.gaf@gmail.com mobarokhossin1@gmail.com mohit.k.misra@gmail.com	Nixxesolutions@gmail.com osacken@gmail.com priyamod345@gmail.com rabsdigital2021@gmail.com rajmnc@gmail.com rustamchik20220504@gmail.com shouserealty@gmail.com sunilramchandani1@gmail.com tairusm@gmail.com tarkdomain@gmail.com uk.dubai81@gmail.com umermian057@gmail.com united.offshore.procurement@gmail.com virildar@gmail.com waqasbaberp@gmail.com wgviagens.hostgator@gmail.com 7862005@yahoo.com ramosoflagosrealty@yahoo.com alez90@yandex.ru ru@yandex.ru sergey@yandex.ru stskuridin@yandex.ru dillu@hotmail.com obaid2283@hotmail.com uruguayamethyst@hotmail.com mohammed.sa3d.uae@gmail.com mydomains99552@gmail.com
---	--



Screenshot of the administrator endpoint on the template



Screenshot of the directory listing present on these websites



We Predict Cyber Threats

Initial Attack Vector Protection Platform

Founded in
2015

200+
CloudSters

2 Offices
HQ in Singapore
and R&D in India

170+
Clients Globally

4
Products

We secure some of the Fortune 500 and Unicorns



... And we are backed by eminent investors



Accelerated by



CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services. We have been featured in several Gartner market guides and are a **qualified AWS partner**.

We are the **Highest Rated Security Threat Intelligence company** on Gartner Peer Insights from the Asia Pacific region.



About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give context to our customers' digital risks.



www.cloudsek.com
info@cloudsek.com