Tracking Adversaries: UAC-0050, Cracking The DaVinci Code

blog.bushidotoken.net/2024/03/tracking-adversaries-uac-0050-cracking.html

BushidoToken

In this blog, we shall investigate a Russia-based mercenary group that has appeared in multiple CERT-UA reports after sending waves of spam to Ukrainian organisations. These mercenaries use tried and tested tactics, techniques, and procedures (TTPs) that are low effort, but operationally functional.

This includes use of off-the-shelf commodity crimeware as well as legitimate remote management and monitoring (RMM) tools. These mercenaries also are notable as they have low operational security (OPSEC) and offer their services publicly, to Russians, via Facebook, Instagram, Telegram, various cybercrime forums, as well as their own websites.

Background on UAC-0050

A report by the Computer Emergency Response Team of Ukraine (CERT-UA) on 22 February 2024 shared a notable statement of attribution to a threat group tracked as UAC-0050 that CERT-UA has shared updates on several times already. The CERT-UA team and other security researchers online believe that UAC-0050 is linked to a Russian-speaking mercenary organization called “The DaVinci Group” or as you will see later on “Agency DaVinci,” or “DaVinci Project.” CERT-UA assessed that UAC-0050 (The DaVinci Group) has ties to Russian law enforcement and has been targeting Ukrainian organizations since the beginning of the Russian invasion of Ukraine in 2022.

CERT-UA say they have attributed at least 15 malicious spam (malspam) campaigns to the DaVinci Group and assess that they are acting as initial access brokers (IABs) for more serious threat groups, potentially the likes of Sandworm (UAC-0082), Fancy Bear (UAC-0028), or Armageddon Group (UAC-0010), among others. The adversaries also are said to deliver up to five different malware families as well, which includes Remcos RAT, Quasar RAT, Venom RAT, RemoteUtilities RMM, and LummaStealer. The notable aspect about these malware families is that they are all off-the-shelf commodity crimeware, which anyone can purchase from the cybercriminal underground with enough Bitcoin.

CERT-UA released several artifacts from malspam campaigns tied to UAC-0050 that are relevant to The DaVinci Group on several occasions:

- On 30 November 2023, they shared a File Path and EXE linked to UAC-0050:
  "%PROGRAMDATA%\Davinci\8161.exe"
- On 13 November 2023, they shared, a File Path and EXE, as well as email and domain linked to UAC-0050:
  - "%PROGRAMDATA%\davinci\sql.exe"
  - info[@]davincigroup[.]online
  - groupdavinci[.]online
- On 22 January 2023, they shared a domain linked to UAC-0050:
  8161[.]uk

Adversary and Victims

Active since at least 2017, but potentially earlier, The DaVinci Group (aka UAC-0050) has recently been launching wave after wave of malspam against Ukrainian targets. Their victims likely range from government ministries, local authorities, the Ukrainian military, and civilians caught in the malspam cross fire, analogous to Russia's war of aggression itself.

Capabilities and Infrastructure

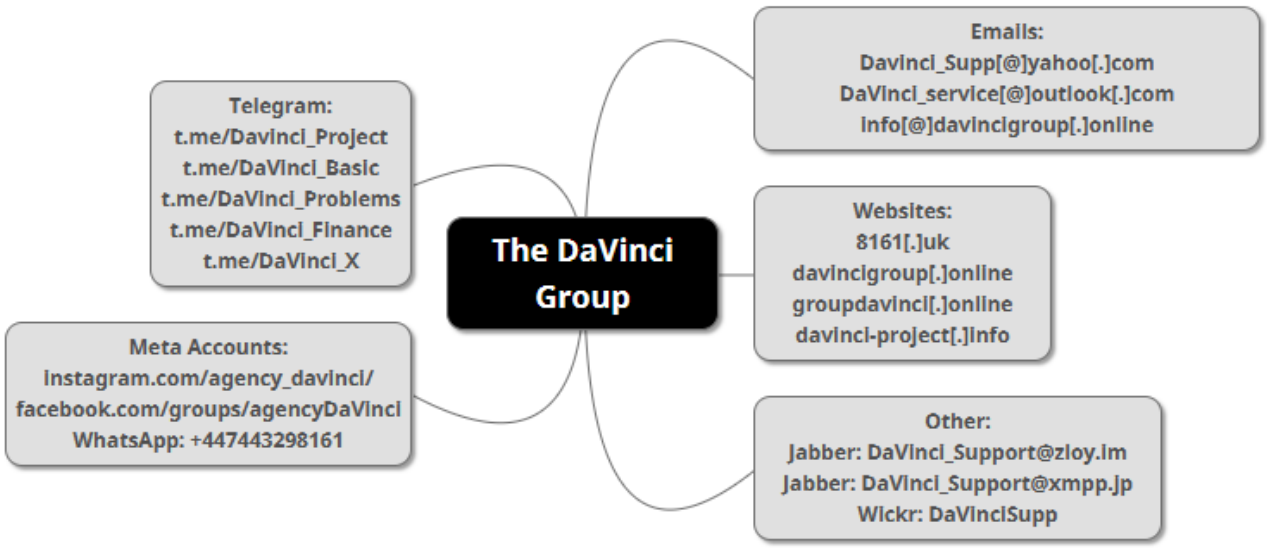
The DaVinci Group (aka UAC-0050) has harvested (or paid for) tens of thousands of Ukrainian email addresses and, as described by CERT-UA, uses them to launch malspam campaigns.

In November 2023, emails sent by DaVinci were delivered to more than 15,000 addresses using a compromised account of one of the judicial authorities of Ukraine. The subject of the email was "Subpoena" making targets think they were being investigated by the law, but instead a RAR file attached to the email contained Remcos RAT instead. Also in November 2023, DaVinci sent another wave of malspam masquerading as the Security Service of Ukraine, that also had a RAR file attached containing Remcos RAT.

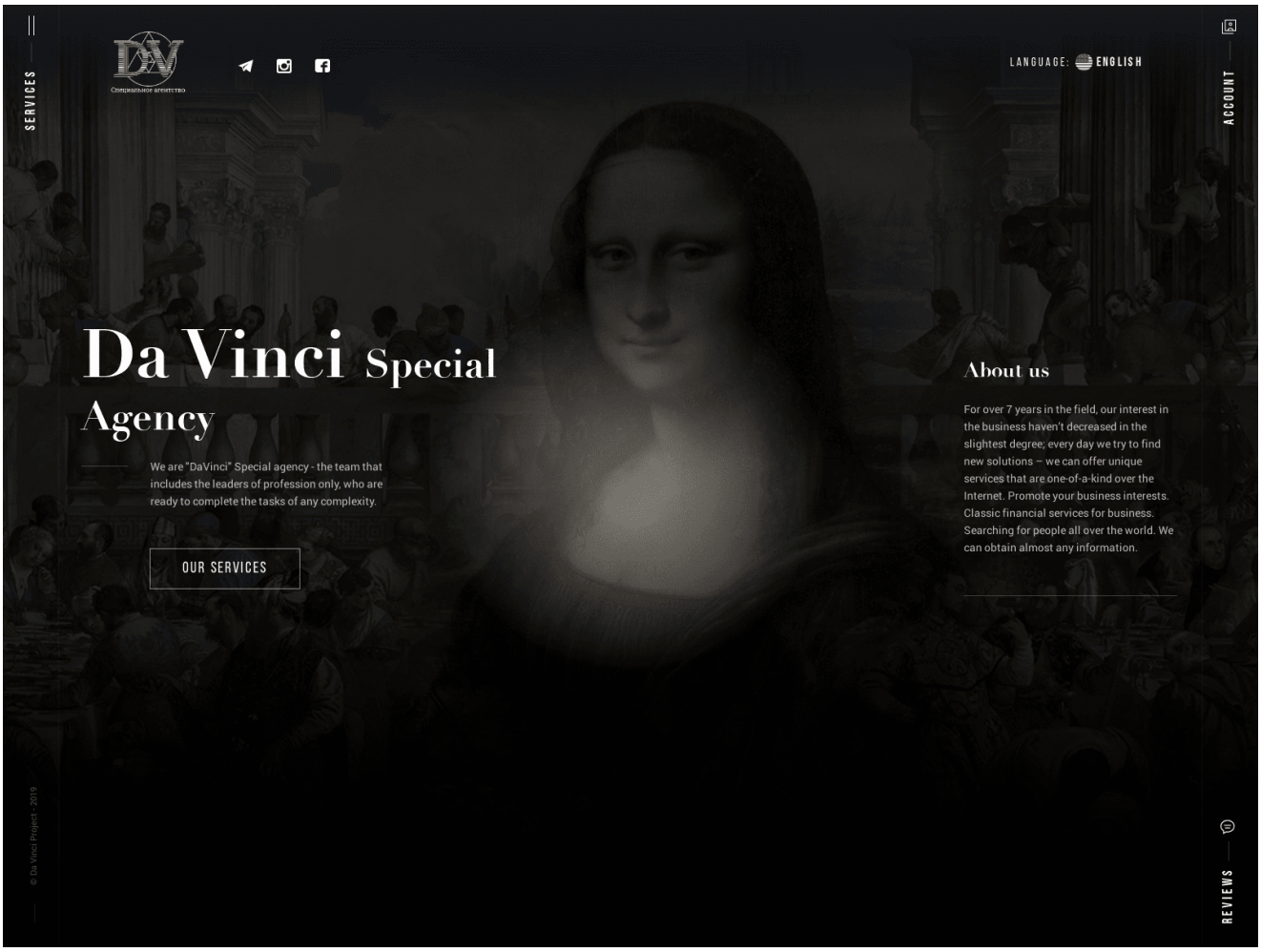
In January 2024, however, DaVinci modified their mass distribution of emails, this time, posing as the State Special Communications Service and the State Emergency Service of Ukraine, which had a link to Bitbucket or RAR file attached that contained the RemoteUtilities legitimate RMM tool. According to the Bitbucket repo's stats, the RemoteUtilities RMM tool was staggeringly downloaded more than 3,000 times in less than 12 hours.

Investigating The DaVinci Group

The artifacts shared by CERT-UA were useful to pivot off of, as well as the fact that DaVinci operators had seemingly made the mistake of mixing up their own website for use during malspam campaigns. From there, it was simple to pivot and uncover their details as they were promoted openly:



The domain 8161[.]uk is The DaVinci Group's main website, whereby they advertise their services, such as hacking people's email accounts, social media accounts, instant messaging accounts, remote access to PCs, launching Denial of Service (DoS) attacks, wiping files/evidence from other computers, and even they claim to have access to up to 150,000 CCTV cameras in Moscow (see below).


SERVICES
Специальное агентство
LANGUAGE: ENGLISH
ACCOUNT
Da Vinci Special
Agency
We are "DaVinci" Special agency - the team that includes the leaders of profession only, who are ready to complete the tasks of any complexity.
OUR SERVICES
About us
For over 7 years in the field, our interest in the business haven't decreased in the slightest degree; every day we try to find new solutions – we can offer unique services that are one-of-a-kind over the Internet. Promote your business interests. Classic financial services for business. Searching for people all over the world. We can obtain almost any information.
© Da Vinci Project - 2019
REVIEWS

Access

ACCESS – as one of the most effective ways to search for information. In today's digital world, the vast majority of people have a very naive understanding of online security. By storing their "secrets" on electronic media, they make our job of finding the information we need very, very easy. Mailboxes, social networks, instant messengers - for 99% of people this is a "closet with skeletons". We can help with access to almost any information.

Now some specifics:

- Access to mail account (MAIL/YANDEX/GMAIL/YAHOO)
- Access to social network (VK/FB/INST)
- Access to CCTV cameras (more than 150,000 only in Moscow and Moscow time)
- Access to instant messengers (VIBER/WHATSAPP/TELEGRAM)

Access to CCTV cameras (more than 150,000 only in Moscow and Moscow time)

LANGUAGE: RUSSIAN CONTACTS

Access to instant messengers (VIBER/WHATSAPP/TELEGRAM)

Before complex tasks:

- Remote access to mobile/computer
- Archives and mirrors of a large number of resources
- Disruption/stopping of the site
- "Excavating" data, "cleaning" traces
- Any actions possible within the framework of operational intelligence activities (operational investigative activities)

All operations take place authorized, without violating the laws of the Russian Federation.

SERVICES

CABINET

REVIEWS

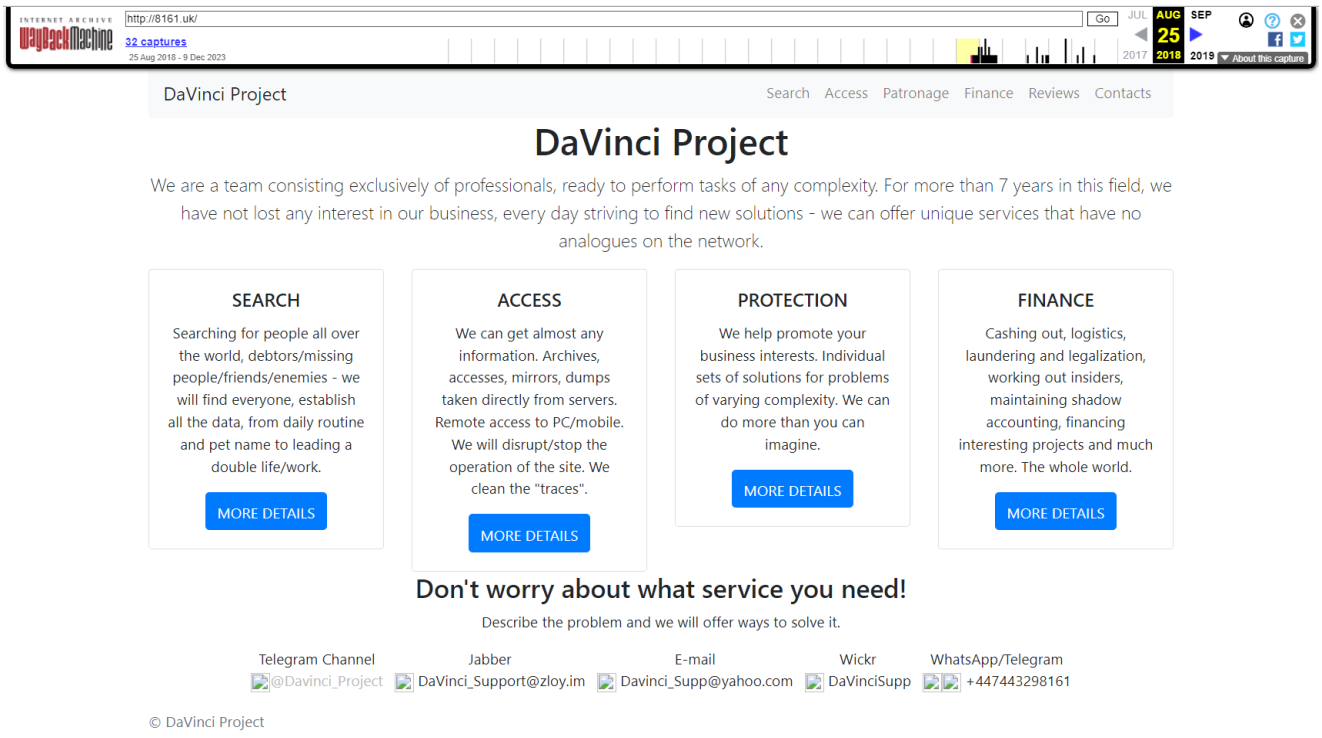
© Da Vinci Project - 2019

SERVICES

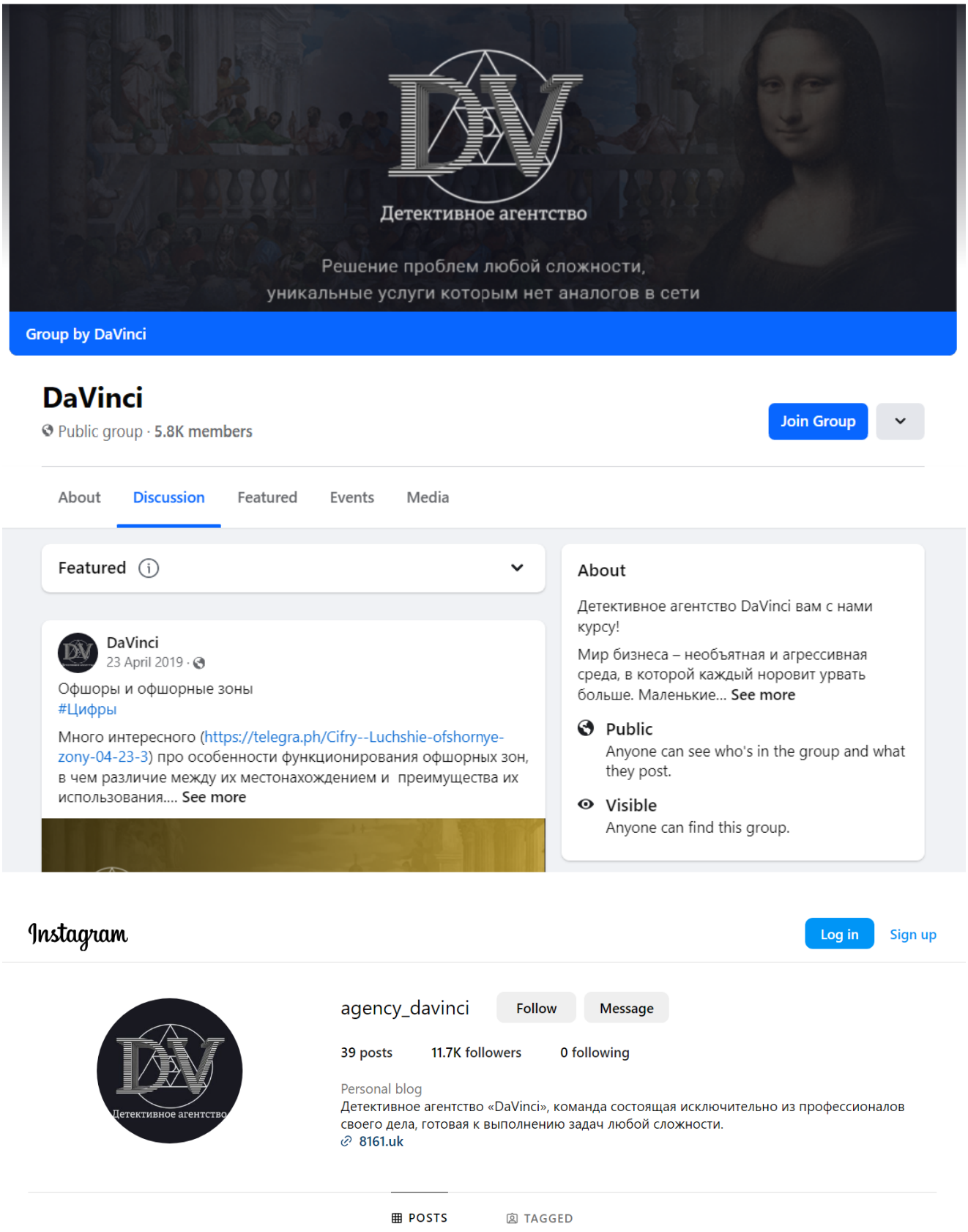
CABINET

REVIEWS

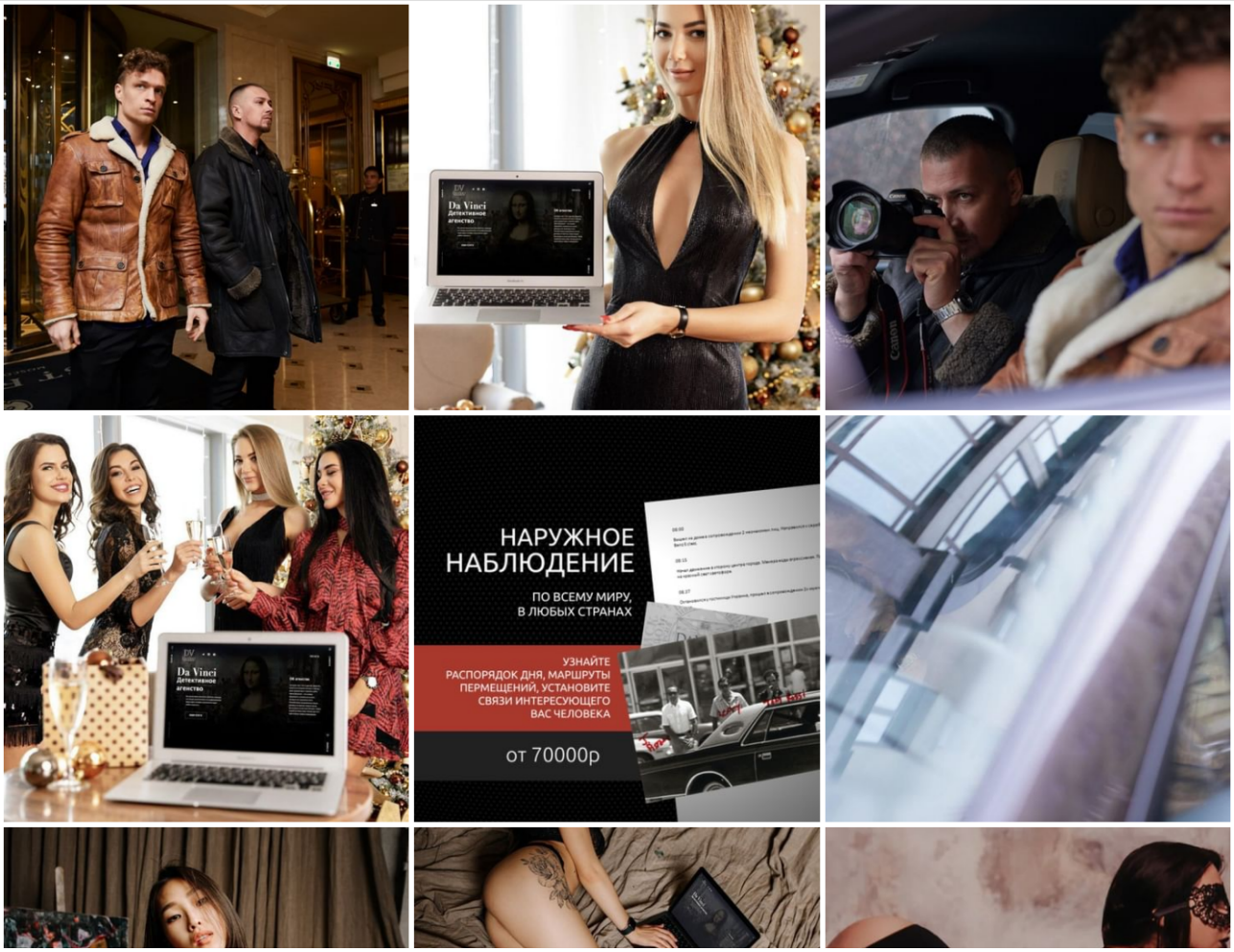
The main “DaVinci Project” website appears to have been around since at least 25 August 2018 and is also connected to other domains such as davincigroup[.]online, groupdavinci[.]online, and davinci-project[.]info.



The website also contains various links to other profiles on social media sites, such as Facebook and Instagram (see below).



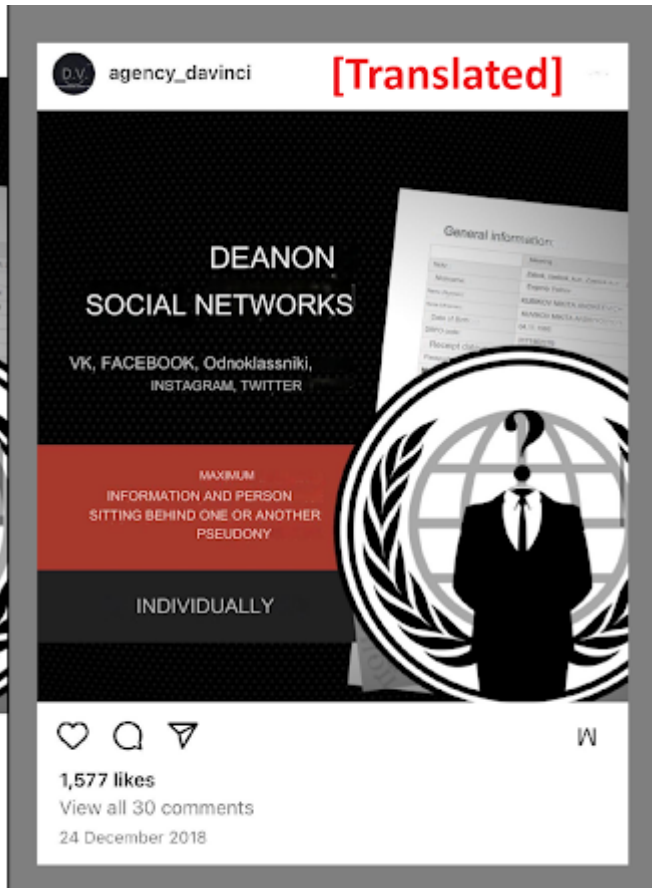
The DaVinci Group's Instagram account also laughably uses absurd marketing tactics such as hiring scantily-clad Russian models to hold up a laptop with their website open. Only in Russia!

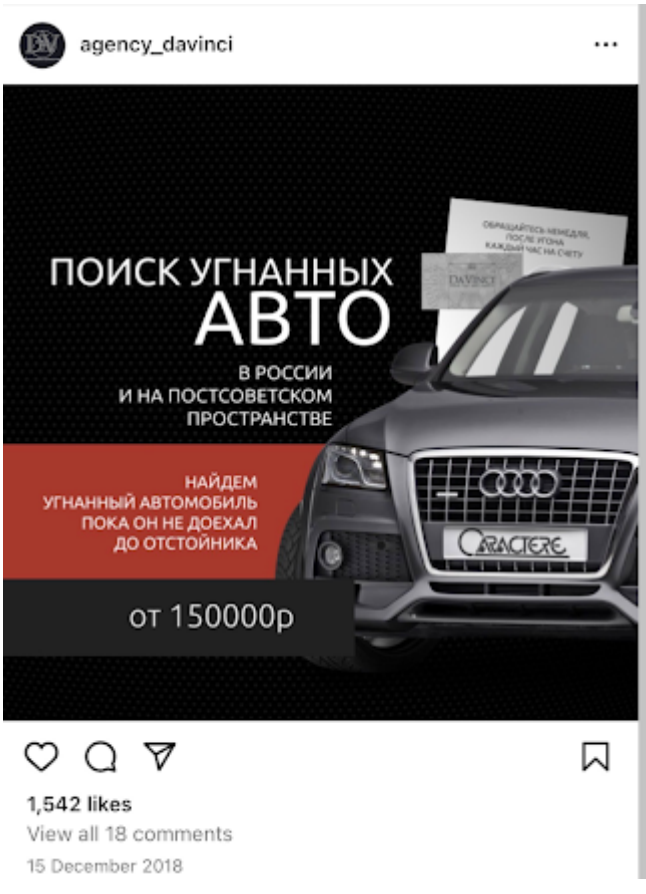


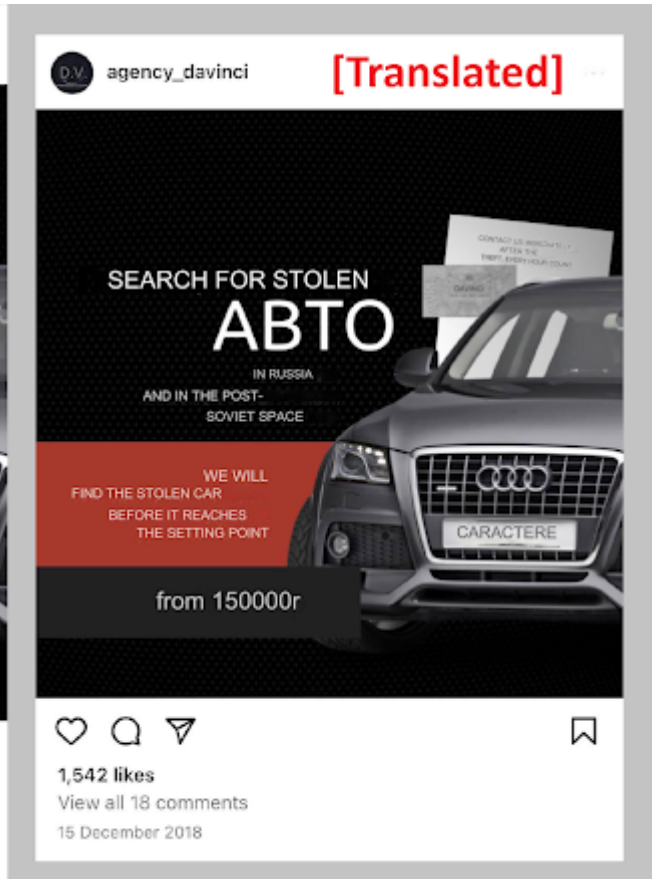
The DaVinci Group's Services

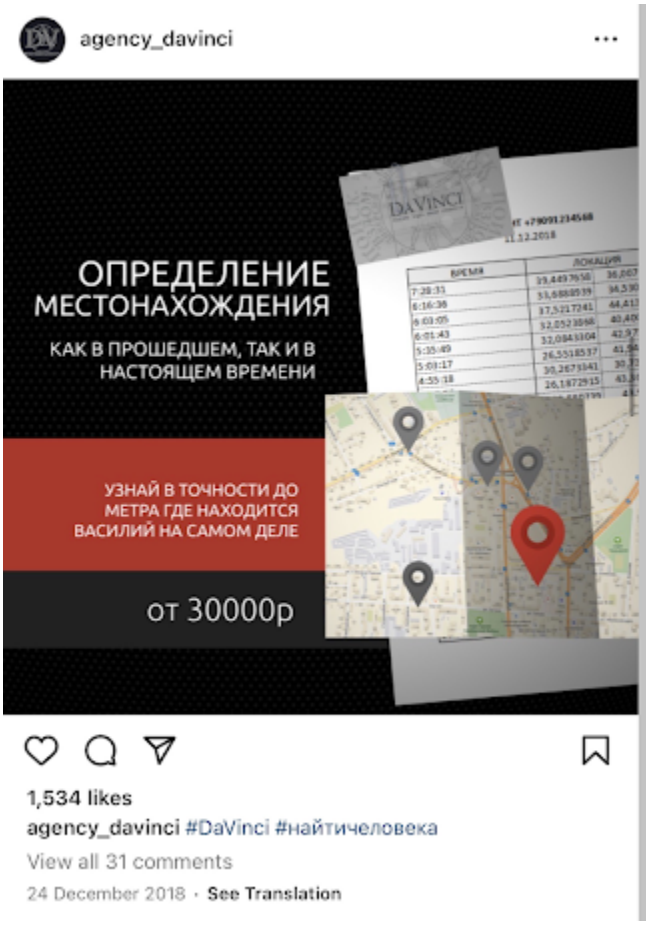
On Instagram, DaVinci had many explicit ads like the above, but they also teased some of their actual hacking, surveillance, and private investigation work too. This included services such as deanonymizing people on social networks, searching for stolen cars online, geolocating people, and physical surveillance (disclaimer: these were machine translated from Russian).

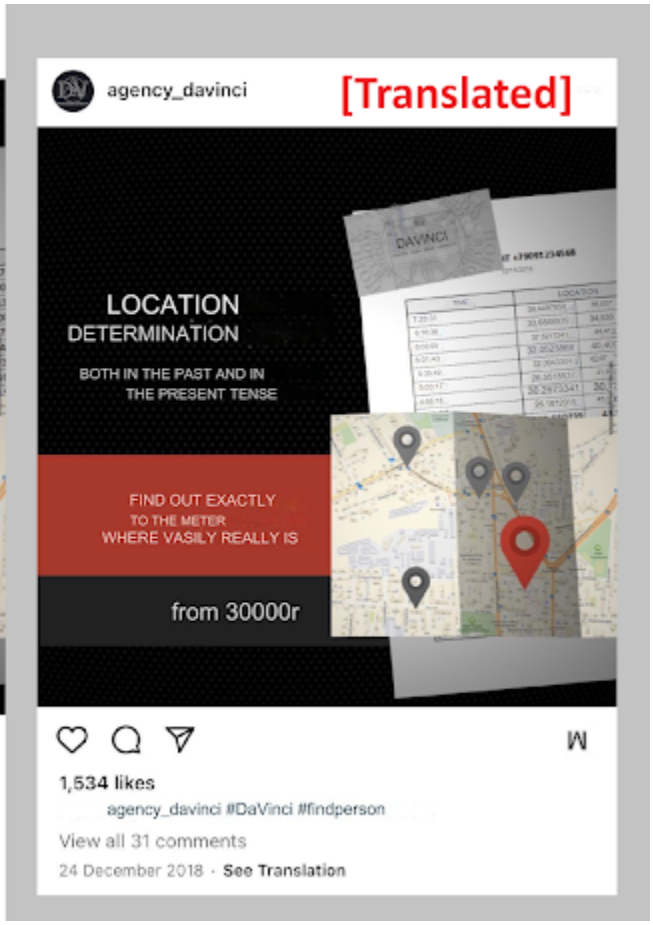

agency_davinci
ДЕАНОН
СОЦ СЕТЕЙ
ВК, ФЕЙСБУК, ОДНОКЛАССНИКИ,
ИНСТАГРАММ, ТВИТТЕР
МАКСИМАЛЬНО
ИНФОРМАЦИИ И ЧЕЛОВЕКЕ
СИДЯЩИМ ЗА ТЕМ ИЛИ ИНЫМ
ПСЕВДОНИМОМ
ИНДИВИДУАЛЬНО
1,577 likes
View all 30 comments
24 December 2018

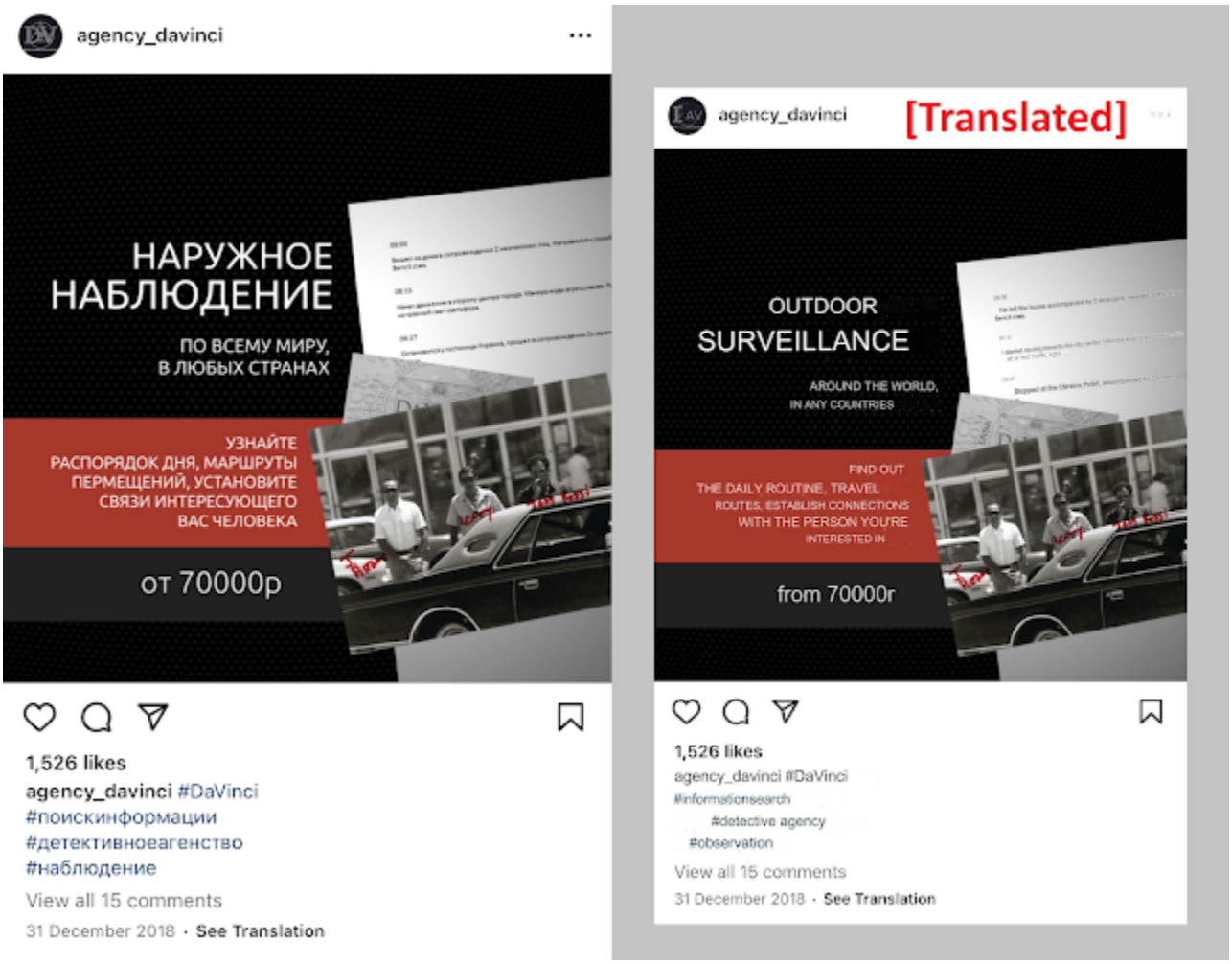

agency_davinci
[Translated]
DEANON
SOCIAL NETWORKS
VK, FACEBOOK, Odnoklassniki,
INSTAGRAM, TWITTER
MAXIMUM
INFORMATION AND PERSON
SITTING BEHIND ONE OR ANOTHER
PSEUDONY
INDIVIDUALLY
1,577 likes
View all 30 comments
24 December 2018


agency_davinci
ПОИСК УГНАННЫХ
АВТО
В РОССИИ
И НА ПОСТСОВЕТСКОМ
ПРОСТРАНСТВЕ
НАЙДЕМ
УГНАННЫЙ АВТОМОБИЛЬ
ПОКА ОН НЕ ДОЕХАЛ
ДО ОТСТОЙНИКА
от 150000р
1,542 likes
View all 18 comments
15 December 2018

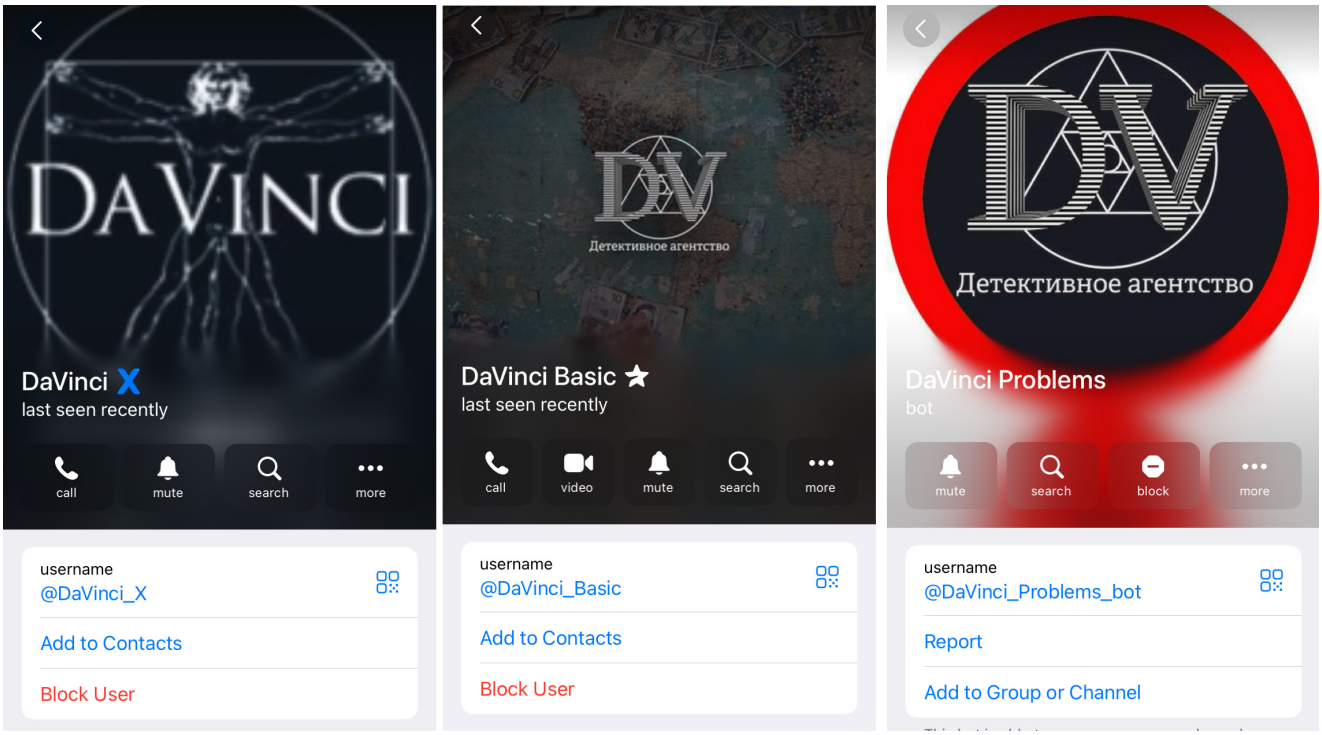

agency_davinci
[Translated]
SEARCH FOR STOLEN
АВТО
IN RUSSIA
AND IN THE POST-
SOVIET SPACE
WE WILL
FIND THE STOLEN CAR
BEFORE IT REACHES
THE SETTING POINT
from 150000r
1,542 likes
View all 18 comments
15 December 2018


agency_davinci
ОПРЕДЕЛЕНИЕ
МЕСТОНАХОЖДЕНИЯ
КАК В ПРОШЕДШЕМ, ТАК И В
НАСТОЯЩЕМ ВРЕМЕНИ
УЗНАЙ В ТОЧНОСТИ ДО
МЕТРА ГДЕ НАХОДИТСЯ
ВАСИЛИЙ НА САМОМ ДЕЛЕ
от 30000р
1,534 likes
agency_davinci #DaVinci #найтичеловека
View all 31 comments
24 December 2018 · See Translation


agency_davinci
[Translated]
LOCATION
DETERMINATION
BOTH IN THE PAST AND IN
THE PRESENT TENSE
FIND OUT EXACTLY
TO THE METER
WHERE VASILY REALLY IS
from 30000r
1,534 likes
agency_davinci #DaVinci #findperson
View all 31 comments
24 December 2018 · See Translation



The way prospective clients contact The DaVinci Group and acquire their services appears to mainly be via Telegram as they have several Telegram accounts related to conducting businesses and there were on the Contact Us page of their website.



DaVinci Mercenaries on the Cybercrime Underground

Interestingly, these semi-professional looking mercenaries advertise a lot on the cybercrime underground forums and various Telegram group chats too. In their cybercrime forum posts, their profiles, often called 'Davinci Assistant' will share a list of their services and prices (see below).

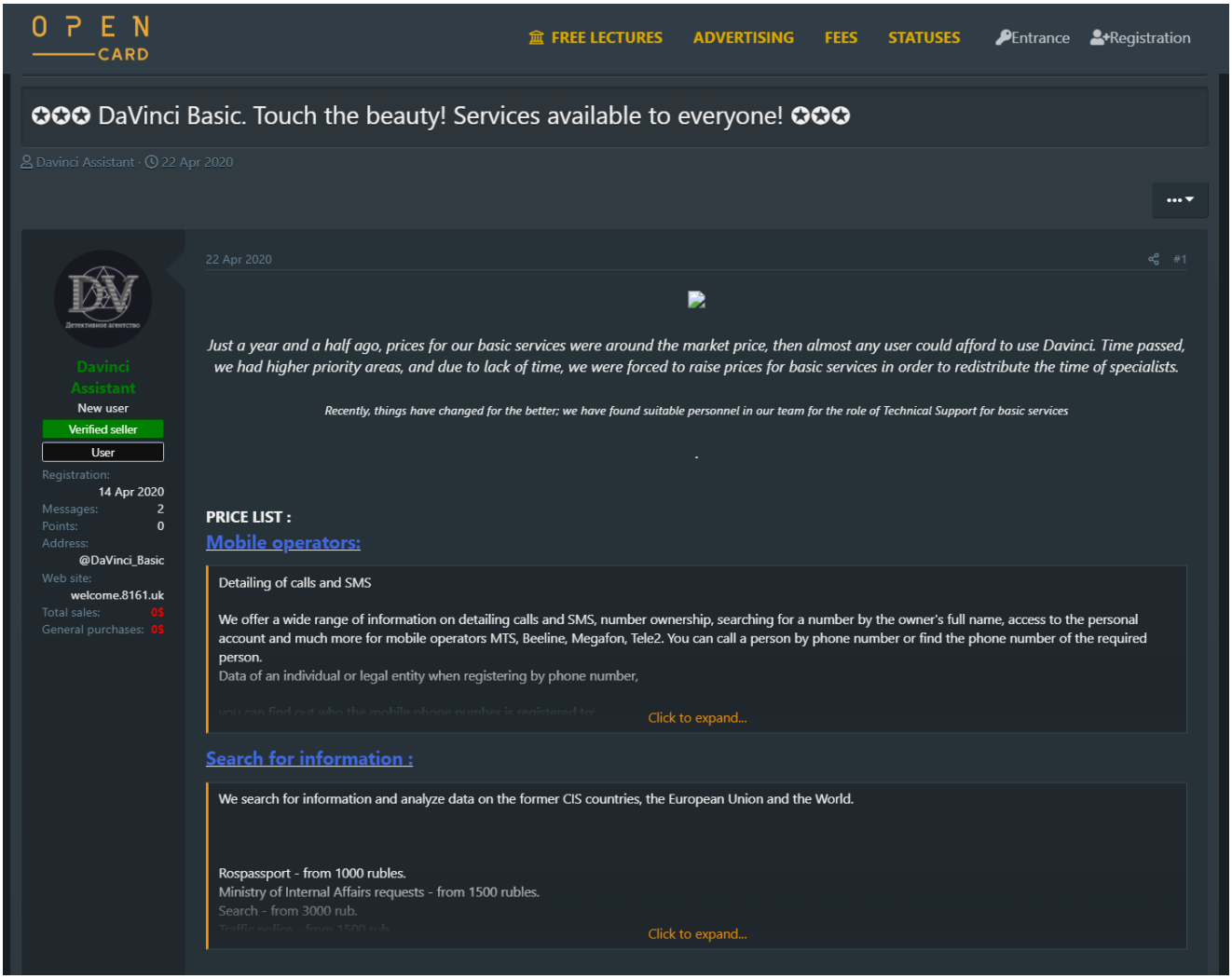
The earliest forum post from DaVinci that could be found was from 28 November 2017 on the now defunct Russian-speaking site BestDarkForum[.]cc. Whereby, DaVinci listed their services such as:

- "Breaking into whatsapp/viber - 350,000 roubles parallel access with correspondence archive."
- "VK architecture with remote messages - 500,000 rubles exclusive from VKontakte servers."
- "Breaking into TV is from 500,000p."
- "Pk/mobile break-in - 150,000p."
- "Stealing social network/messenger accounts from 100,000p."
- "Gmail archive - 250,000p."
- "Corporate mail, 150,000p."
- "Withdrawal of info from cellular towers - from 300 000p"
- "Interception of Internet traffic - from 400,000p"
- "Monitoring cell phone movements - from 900,000p per week"
- "Search for stolen cars - 200 000p"
- "Establishment/elimination of exit/entry ban – 100,000p"
- "Telegram hacking - 500,000p"

To put these prices into perspective, 100,000 Russian Rubles roughly equals 865 British Pounds. The official symbol of the Russian currency is ₽, but 'p' is also used colloquially.

DaVinci Mobile SIM Hacking

A more recent post on the Russian-speaking forum Open Card, on 22 April 2020, saw the DaVinci group offering a range of other services, potentially indicating they have insiders or abuse of police powers at various Russian mobile carriers and telecommunications companies.



Some of these services were as follows:

Data of an individual or legal entity when registering by phone number, you can find out who the mobile phone number is registered to:

- Beeline - from 1000 rubles
- MTS - from 1500 rub.
- Megafon - from 2000 rub.
- Tele2 - from 5000 rub.
- Yota - from 5000 rub.

Details of calls and SMS of an individual (without text) without base station addresses:

- Beeline - from 3000 rub. for 1 month
- MTS - from 15,000 rubles. for 1 month
- Megafon - from 15,000 rubles. for 1 month
- Tele2 - from 13,000 rubles. for 1 month
- Yota - from 30,000 rubles. - from 1 month

Access to an individual's personal account:

- Beeline - from 25,000 rubles.
- MTS - from 35,000 rub.
- Megafon - from 35,000 rub.
- Tele2 - from 50,000 rub.
- Yota - from 70,000 rub.

Blocking a phone number:

- Beeline - from 7,000 rubles.
- MTS - from 8000 rub.
- Megafon - from 9000 rub.
- Tele2 - from 15,000 rub.
- Yota - from 20,000 rub.

Additional mobile-hacking related services:

- SMS details with text for 1 month: Any operator in the Russian Federation - from 150,000 rubles.
- Flash, any operator in the Russian Federation (all operators) - from 40,000 rubles.
- Marking call points on the map via BS per month (all operators) - from 10,000 rubles.

Other notable services offered by DaVinci via their Open Card post were as follows:

- Comprehensive dossiers on Phys. persons - from 20,000 rubles, Legal entity. persons - from 30,000 rubles
- Ministry of Internal Affairs (Russia) requests - from 1500 rubles.
- Interpol Search - from 50,000 rub.
- Europol Search - from 80,000 rub.
- Weapons (Registered weapons on a citizen) Search - from 5,000 rubles.
- Crossing the border Search - from 11,000 rubles.
- Flight Passenger list - from 10,000 rubles.
- Determine data on IP - from 100,000 rubles.
- Bank Account balance (balance) - from 20,000 rubles.
- Addresses of ATMs used by the target - from 30,000 rubles/month

This type of service offered by DaVinci is also known as "Probiv", which is a Russian-language slang term best translated to English as “look-up”. This is where a customer can provide some info of an individual and can get other personal information associated with the target, for a fee. Acquiring this data is believed to be largely facilitated by corrupt Russian employees using their privileged position to perform searches on internal systems to obtain data requested by the cybercrime forum vendors (in this case, DaVinci), who act as intermediaries.

Conclusion

The reports by CERT-UA on UAC-0050 lead us to believe that The DaVinci Group mercenaries are potentially working with Russian government to target Ukraine. From investigating DaVinci’s services on their websites, social media posts, and cybercrime forum posts, it appears that they have the capabilities to do so.

However, the sheer lack of OPSEC by using their own branded website as a command-and-control (C2) server is unusual. CERT-UA did also note this odd behaviour and mentioned in their report that The DaVinci Group has “recently been actively trying to draw attention to themselves” as well.

One hypothesis for this bizarre activity could be that DaVinci may even be using CERT-UA’s incident reports as a sort of meta advertising tool to get themselves noticed by Russian intelligence agencies, trying to win a big contract to act as initial access brokers for Russian APT groups such as Sandworm, Turla, or CozyBear, which are affiliated with the GRU, FSB, and SVR, respectively.

In closing, The DaVinci Group (UAC-0050) is a low tier mercenary threat group that appears to dabble in cybercrime and state-sponsored intelligence gathering. The very existence of this threat group further highlights the blurred lines between cybercrime underground and the Russian government.

Raspberry Robin: A global USB malware campaign providing access to ransomware operators

Tracking Adversaries: Scattered Spider, the BlackCat affiliate

Lessons from the iSOON Leaks