BEYOND DONATIONS: HOW HACKTIVIST GROUPS FUND THEIR OPERATIONS

KELA

Beyond Donations: How Hacktivist Groups Fund Their Operations

KELA Cybercrime Intelligence Center

Table of Contents

Executive summary **2**
Introduction **3**
Killnet funding attempts **6**
"Private Military Hacking Company" 7
"Dark School" - Killnet's training program 9
Killnet's Cryptocurrency exchange 10
Investor funding 11
Selling of data, accesses, and logs 12
Ransoms 14
Infinity forum 16
Anonymous Russia **18**
Tesla-Botnet 18
DDoS TOR service 18
Phoenix **21**
Selling of stolen data 21
Ransoms 21
Selling training 23
DDoS-for-hire services 24
Streaming attacks 25
Anonymous Sudan **26**
Selling of stolen data 27
Ransom DDoS attacks 30
Arvin Club **32**
Subscription-based Telegram channel 32
Advertising 32
Selling data 33
Other groups **34**
Conclusion **35**

Executive summary

2022 saw a dramatic increase in hacktivist activity, largely sparked by the Russia-Ukraine conflict, but also by other geo-political tensions. The hacktivist groups are not conducting their attacks for financial gain but rather to cause damage to their victims and to spread their political agenda or social change.

Now, a year and a half into the war, the hacktivist activity has continued. Since March 2022, Killnet has been observed asking for donations to fund their activities, as well as some other hacktivist groups. However, it is becoming apparent that relying on these donations alone is not enough.

In this report, KELA looks at whether hacktivist groups, such as Killnet, Anonymous Sudan, Phoenix and others are looking beyond donations to fund their activities by monetizing their operations.

KELA identified that in 2023 and the latter part of 2022, hacktivist groups have been seen using different methods to source income, including:

- Selling stolen data, accesses, and logs
- Selling training courses
- Attempting to extort ransoms from their victims
- Selling botnet licenses
- Looking for investor funding for their projects
- Selling advertisement spaces
- Providing hack-for-hire services

These groups' attempts at monetizing their operations do demonstrate that they want to stay active even if donations are not sufficient enough to support their activities (as stated by Killnet on several occasions). In this report, KELA explores the success of these attempts and assesses whether these monetization efforts considerably increase or change the threat posed by these groups.

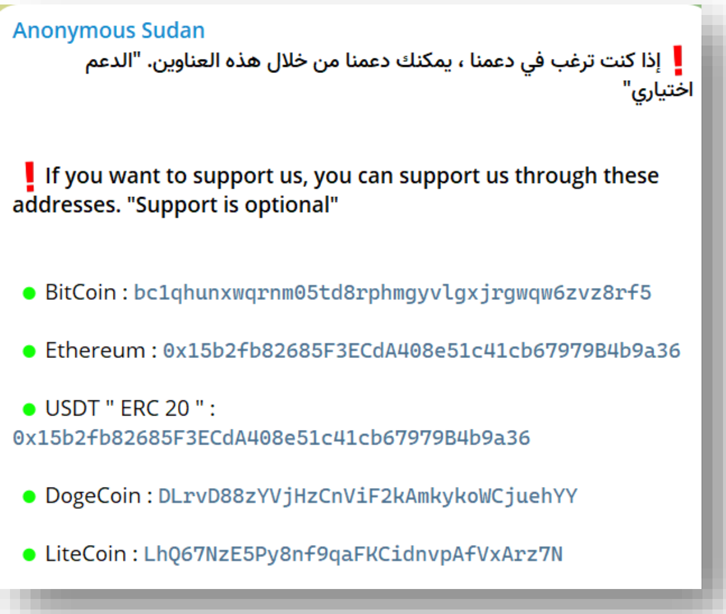
Introduction

Hacktivists are groups or individuals who conduct attacks in support of their political, social, or religious beliefs. They are often looking to raise awareness and bring attention to causes they deem important. Hacktivists target a range of entities that they believe have done wrong, including government organizations, multinational corporations, religious organizations, or even terrorists and drug dealers.[1] Denial of service attacks, website defacement, leaking stolen information, doxing and deploying ransomware are all among the types of attacks that have been used by different hacktivist groups.[2]

In 2022, the Russia-Ukraine conflict resulted in a significant increase in hacktivist activity, with new groups emerging and existing groups re-emerging. In particular, pro-Russian actors have emerged targeting not only Ukraine but all the countries supporting Ukraine in its war with Russia. Although financial gain is not these groups' motivation, money is required to fund their activities. Due to their beliefs and actions closely aligning with the Russian government, it is believed that some of these groups are state-affiliated. However, these groups deny their affiliation with the Russian government and there is no proof they receive substantial funding from the government.

Various hacktivist groups have been observed asking for donations to fund their activities. For example, pro-Russian Killnet, Anonymous Russia, Anonymous Sudan, BloodNet and Phoenix have all, in at least a couple of instances, posted to their Telegram channels asking for donations from their supporters, both in cryptocurrency and "usual" currency.

[1] Fortinet
[2] Fortinet; Twitter



Anonymous Sudan

❗ إذا كنت ترغب في دعمنا ، يمكنك دعمنا من خلال هذه العناوين. "الدعم
اختياري"

❗ If you want to support us, you can support us through these addresses. "Support is optional"

● BitCoin : bc1qhunxwqrnm05td8rphmgyvlgxjrgwqw6zvz8rf5

● Ethereum : 0x15b2fb82685F3ECdA408e51c41cb67979B4b9a36

● USDT " ERC 20 " :
0x15b2fb82685F3ECdA408e51c41cb67979B4b9a36

● DogeCoin : DLrvD88zYVjHzCnViF2kAmkykoWCjuehYY

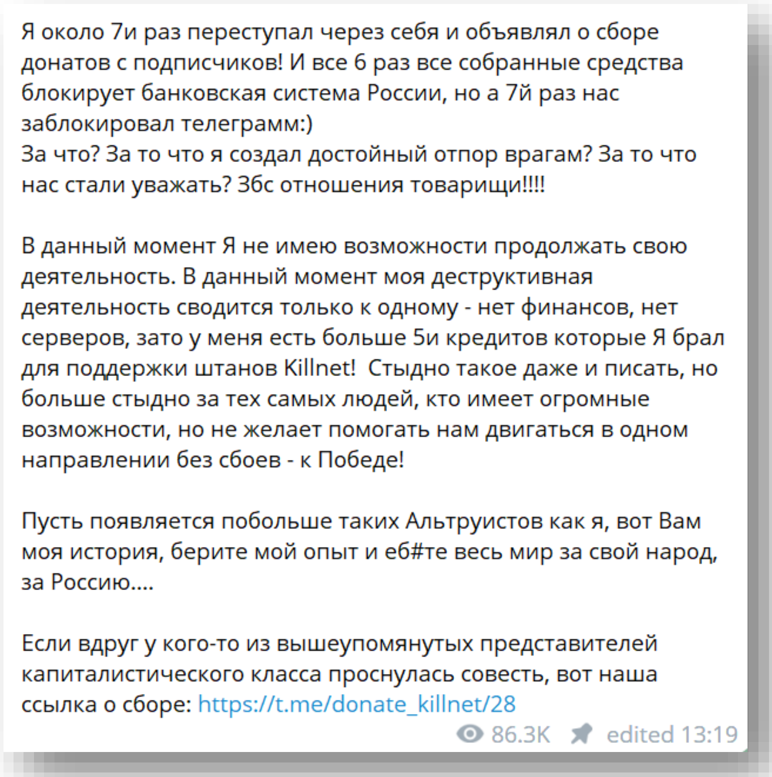
● LiteCoin : LhQ67NzE5Py8nf9qaFKCidnvpAfVxArz7N

Anonymous Sudan asks for donations

KELA reviewed some of the recent Bitcoin wallets shared to Killnet's Telegram channel in posts asking for donations. KELA identified that there were incoming transactions to these wallets, however, it cannot be confirmed that these transactions were in fact donations. These transactions ranged in value from a couple of dollars to a couple of hundred dollars. In certain instances, KELA could identify incoming transactions on the same day that Killnet shared the wallet asking for donations.

For instance, on September 27, 2022, Killmilk, the leader of Killnet, announced that they were unable to continue their activities due to a lack of finances. A few days later Killnet resumed their operations, expressing gratitude for the support from some followers. KELA identified that more than USD 700 was transferred to one of the wallets shared by Killnet on the same date they announced the suspension of their activities.[3] These transactions, although unconfirmed, could have been donations from supporters.

[3] Blockchain



Я около 7и раз переступал через себя и объявлял о сборе донатов с подписчиков! И все 6 раз все собранные средства блокирует банковская система России, но а 7й раз нас заблокировал телеграмм:)
За что? За то что я создал достойный отпор врагам? За то что нас стали уважать? Збс отношения товарищи!!!!

В данный момент Я не имею возможности продолжать свою деятельность. В данный момент моя деструктивная деятельность сводится только к одному - нет финансов, нет серверов, зато у меня есть больше 5и кредитов которые Я брал для поддержки штанов Killnet! Стыдно такое даже и писать, но больше стыдно за тех самых людей, кто имеет огромные возможности, но не желает помогать нам двигаться в одном направлении без сбоев - к Победе!

Пусть появляется побольше таких Альтруистов как я, вот Вам моя история, берите мой опыт и еб#те весь мир за свой народ, за Россию....

Если вдруг у кого-то из вышеупомянутых представителей капиталистического класса проснулась совесть, вот наша ссылка о сборе: https://t.me/donate_killnet/28

Extract of Killmilk post announcing the suspension of their activities due to a lack of finances: "Currently I have no opportunity to resume my activities. Currently my destructive activities are only these — there are no funds, no servers, but there are more than 5 loans I took to support Killnet's pants."

However, are groups looking for other methods, beyond donations, to fund their operations? In 2023 and the latter part of 2022, hacktivist groups tried various methods, some of which are no longer active, to provide an additional income stream to help fund their operations. Methods that have been observed include demanding ransoms from their victims, selling stolen data, selling training courses, and even offering hack-for-hire services.

Despite the apparent effort to explore new income sources, it remains evident that finding alternative funding is not the primary objective of these groups. Instead, the focus remains on activism and spreading their message. It appears that the groups are attempting, sometimes chaotically, to test every possible way for funding their activities, with at least some of these efforts appearing to have been unsuccessful or not gaining the desired attention. The groups' achievements in this field define the future of their hacktivism: will they depend on donations and help from their community or will they transform into more powerful operations?

Killnet funding attempts

Killnet is a pro-Russian hacktivist group that has been targeting organizations from Ukraine and its allies since February 2022. Killnet was founded in November 2021 by the actor ‘Killmilk’. Initially, Killnet was a financially motivated group promoting a botnet for hire. The group switched to hacktivist activities after the outbreak of the Russia-Ukraine conflict.

Since the start of the conflict, Killnet has targeted entities from various countries including Ukraine, Estonia, France, Germany, Italy, Japan, Lithuania, Norway, Poland, Switzerland, the UK, and the US. Most of the group’s activity has been DDoS attacks. Various other groups joined Killnet and collaborated on attacks; currently, the group is in the process of reorganization and is ending its relationships with certain members.

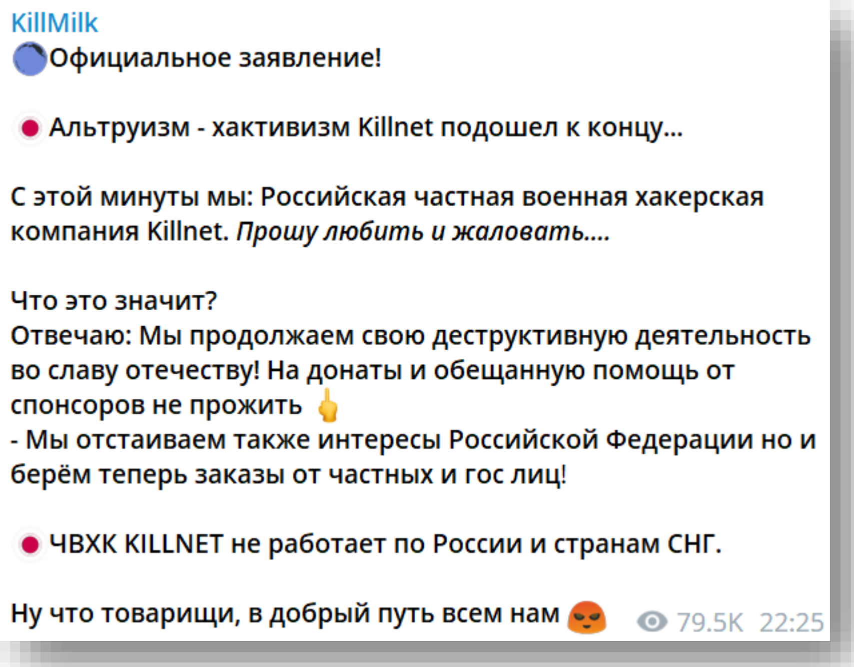
Killnet has been observed engaging in various attempts to earn money, alongside their fundraising, with some efforts still ongoing and others no longer active. Methods used by Killnet include the attempted creation of a private military hacking company, selling goods and services, launching a hacking forum, sourcing funding from investors, demanding ransoms from their victims, and setting up a cryptocurrency exchange.

“Private Military Hacking Company”

Killnet has made several attempts at setting up a private military hacking company in which they would offer mostly hack-for-hire services. However, Killnet shortly reverted back to its hacktivist structure, though it still offers DDoS-for-hire services.

In March 2023, Killmilk announced the formation of Black Skills, a private military hacker company. This appeared to be a side project, rather than a full reorganization of Killnet. However, in April 2023, Killmilk announced the restructuring of Killnet into a private military hacker company, going by the name “ЧВХК KILLNET” (PMHC Killnet). They noted Killnet’s hacktivist activities had come to an end as they cannot survive off donations and help from sponsors alone. It is possible that this restructuring was due to Black Skills not gaining the desired traction, prompting Killnet to transform the whole group in order to bring more attention to the hack-for-hire services.

Amongst the services offered by Killnet were “destructive” attacks against European and US individuals and entities, including disinformation campaigns, attacks on network infrastructure, industrial sabotage, and reputational damage. Other services offered included software development and other non-cyber services to Russian entities, for example, the production of UAVs, though such capabilities of Killnet have been never proven.



KillMilk

🌑Официальное заявление!

🔴 Альтруизм - хактивизм Killnet подошел к концу...

С этой минуты мы: Российская частная военная хакерская компания Killnet. *Прошу любить и жаловать....*

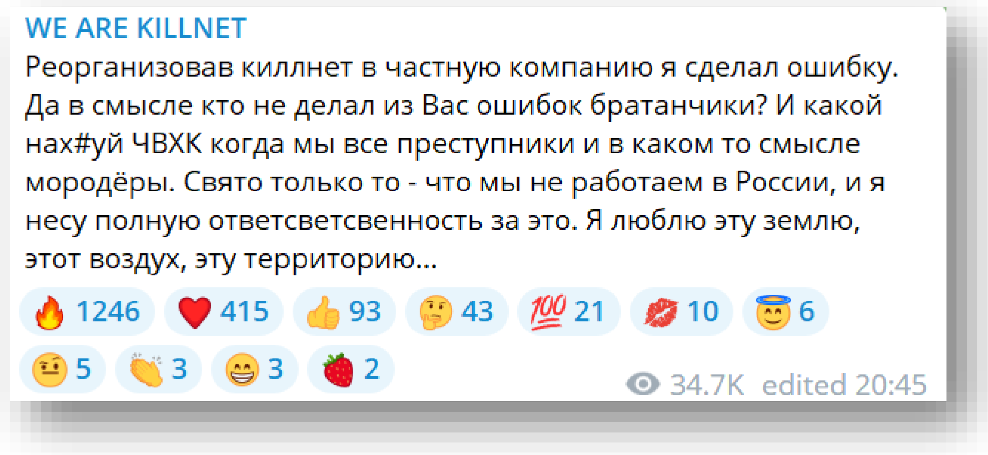
Что это значит?
Отвечаю: Мы продолжаем свою деструктивную деятельность во славу отечеству! На донаты и обещанную помощь от спонсоров не прожить 🖕
- Мы отстаиваем также интересы Российской Федерации но и берём теперь заказы от частных и гос лиц!

🔴 ЧВХК KILLNET не работает по России и странам СНГ.

Ну что товарищи, в добрый путь всем нам 😈 79.5K 22:25

Killmilk announces Killnet’s move to becoming a private military hacking company

Shortly after the announcement of ЧВХК KILLNET, in May 2023, Killnet stated that they had made a "mistake" reorganizing into a private military hacking company. It is unclear why the group backtracked but it could be that they were not receiving the necessary attention or that they did not actually have the skills or resources to provide the services they had advertised. Killnet reverted back to its hacktivist structure by asking for donations from its supporters again.



WE ARE KILLNET

Реорганизовав киллнет в частную компанию я сделал ошибку. Да в смысле кто не делал из Вас ошибок братанчики? И какой нах#уй ЧВХК когда мы все преступники и в каком то смысле мородёры. Свято только то - что мы не работаем в России, и я несу полную ответсветсвенность за это. Я люблю эту землю, этот воздух, эту территорию...

Killnet announces that the restructuring of Killnet into a private military hacking company was a mistake

In July, Killnet announced a new DDoS service. The service will include both layer 7 and layer 4 DDoS attacks, as well as an onion service, although currently only the layer 7 DDoS attack service is available. No prices are provided for the service, with them stating that "prices are discussed individually".

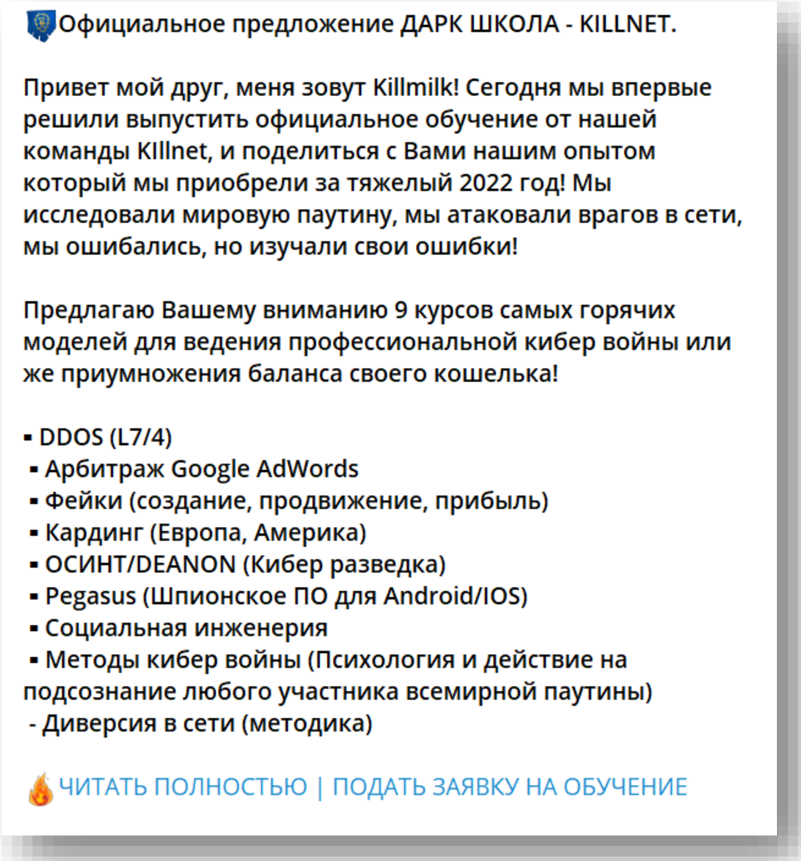
“Dark School” - Killnet’s training program

On April 4, 2023, Killmilk announced Dark School, a training program developed by the Killnet team, consisting of nine courses offered for sale for USD 500 (the first 500 participants could buy the training for USD 249). The course covered various topics including DDoS, carding and social engineering.

Although there were posts on the Dark School Telegram channel suggesting that spots were being filled, there are indications that this course did not achieve the popularity Killnet had hoped for.

In Killmilk’s announcement of Dark School, they noted that training would start after 2000 people had enrolled. The thread on the Killnet-owned Infinity forum did not gain a lot of attention from forum members, with few members showing interest.

The course was intended to be split into two groups, the first set to start on May 10, 2023. However, on the date the course was due to commence, it was announced that due to the number of registered participants, the two groups would be combined into one. Places to attend Dark School were still being advertised on May 12, 2023. The course began on May 25, 2023.



Официальное предложение ДАРК ШКОЛА - KILLNET.

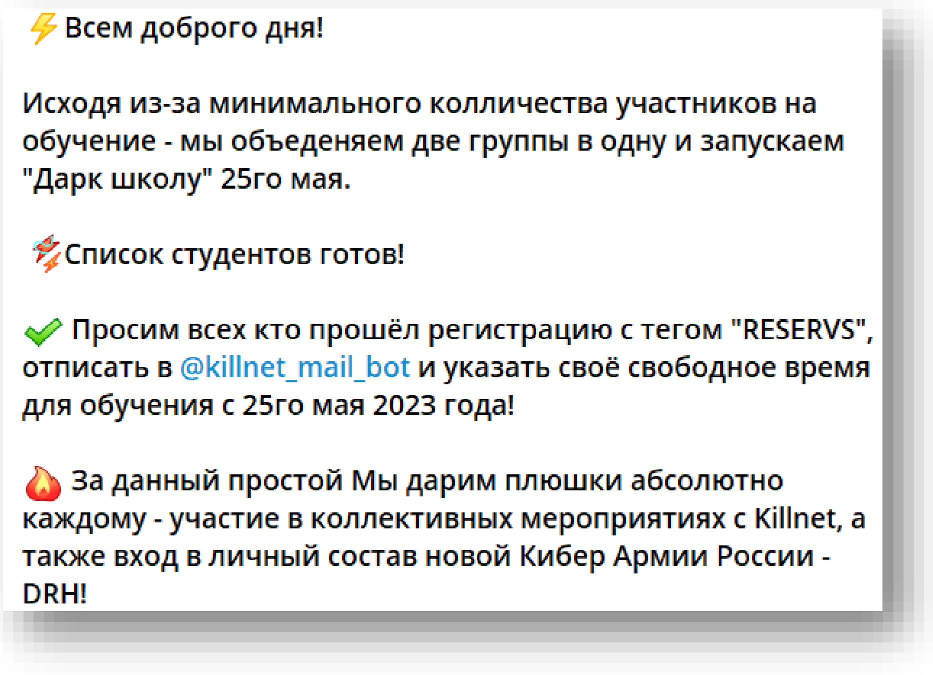
Привет мой друг, меня зовут Killmilk! Сегодня мы впервые решили выпустить официальное обучение от нашей команды KIllnet, и поделиться с Вами нашим опытом который мы приобрели за тяжелый 2022 год! Мы исследовали мировую паутину, мы атаковали врагов в сети, мы ошибались, но изучали свои ошибки!

Предлагаю Вашему вниманию 9 курсов самых горячих моделей для ведения профессиональной кибер войны или же приумножения баланса своего кошелька!

▪ DDOS (L7/4)
▪ Арбитраж Google AdWords
▪ Фейки (создание, продвижение, прибыль)
▪ Кардинг (Европа, Америка)
▪ ОСИНТ/DEANON (Кибер разведка)
▪ Pegasus (Шпионское ПО для Android/IOS)
▪ Социальная инженерия
▪ Методы кибер войны (Психология и действие на подсознание любого участника всемирной паутины)
- Диверсия в сети (методика)

🔥ЧИТАТЬ ПОЛНОСТЬЮ | ПОДАТЬ ЗАЯВКУ НА ОБУЧЕНИЕ

Advertisement of Dark School on Dark School Telegram channel



⚡ Всем доброго дня!

Исходя из-за минимального колличества участников на обучение - мы объеденяем две группы в одну и запускаем "Дарк школу" 25го мая.

🚀Список студентов готов!

✅ Просим всех кто прошёл регистрацию с тегом "RESERVS", отписать в @killnet_mail_bot и указать своё свободное время для обучения с 25го мая 2023 года!

🔥 За данный простой Мы дарим плюшки абсолютно каждому - участие в коллективных мероприятиях с Killnet, а также вход в личный состав новой Кибер Армии России - DRH!

Announcement that the two Dark School training groups will be combined

Another, much smaller scale Dark School course which appears to be on how to abuse Bing Ads for malicious purposes was also advertised on April 17, 2023. The course is for private training for a group of up to 100 participants, costing USD 1149. Some Telegram users commented on the high price of the training, noting that cheaper courses can likely be found elsewhere.

Killnet's Cryptocurrency exchange

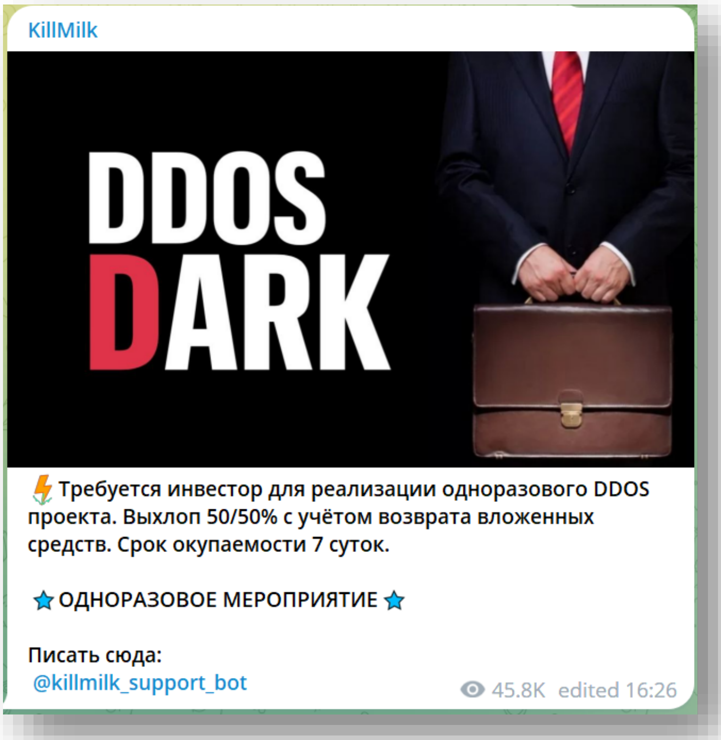
On May 8, 2023, Killnet announced their cryptocurrency exchange where various exchanges can be performed, including cryptocurrency to cash and cryptocurrency to cryptocurrency, at a service rate between 3-4%. The exchange also offers mixer services, allowing to wash cryptocurrency in cash or other cryptocurrency, at a rate of between 3-6% depending on the amount of money.

This is not the first time that Killnet has engaged in cryptocurrency exchange services. They have partnered with another exchange called "Netto_Exchange" since September 2022.

Investor funding

Killnet has also been observed on several occasions looking for investors to help fund their projects. Black Skills was one of Killnet's projects seeking investors, posting on their Telegram channel in March 2023 that they were looking for an investor who could invest at least 5 million into Black Skills (it's not clear, in which currency, but possibly rubles). In return, they would have a 51% stake in Black Skills. The sheer amount of money required from an investor likely minimized the chances of this project being successful and likely contributed to Killnet's backtrack to a hacktivist structure.

Moreover, on February 26, 2023, Killmilk announced that they were looking for an investor to help implement a one-time DDoS project, who will receive 50% of the profits.



KillMilk

⚡Требуется инвестор для реализации одноразового DDOS проекта. Выхлоп 50/50% с учётом возврата вложенных средств. Срок окупаемости 7 суток.

⭐ОДНОРАЗОВОЕ МЕРОПРИЯТИЕ⭐

Писать сюда:
@killmilk_support_bot

45.8K edited 16:26

Killmilk post looking for an investor for a DDoS project

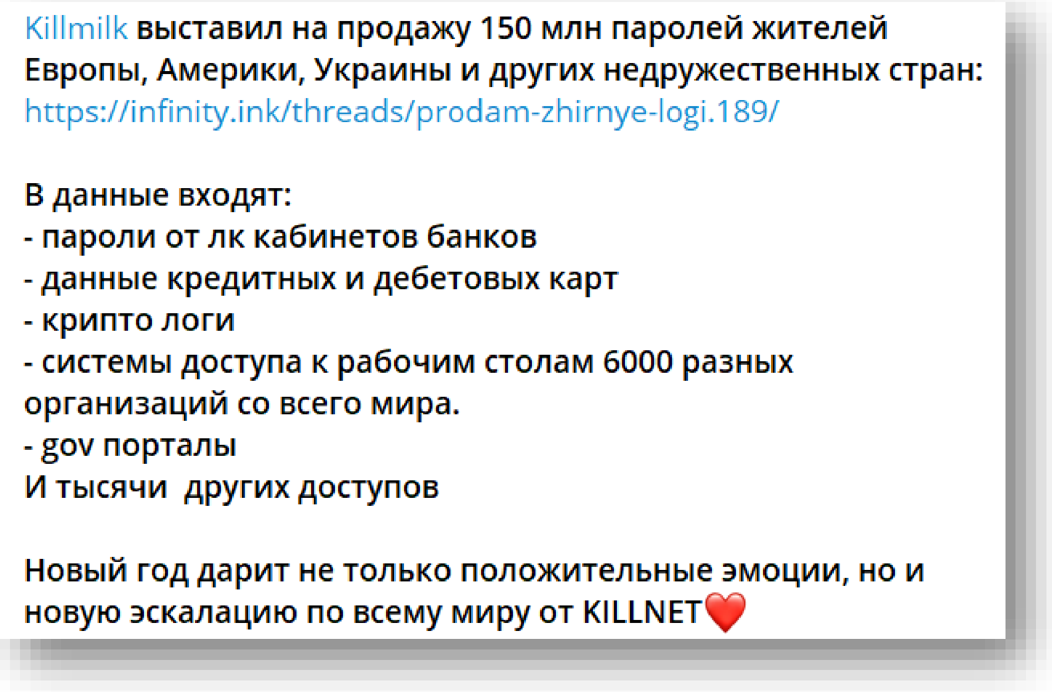
Separately, in a non-cyber related project, Killnet announced on June 9, 2023, the upcoming production of a short film that will focus on the proliferation of Russian hacktivism since February 2022. In addition to looking for participants in the film, they also state that they would be grateful for any sponsors.

Selling of data, accesses, and logs

Killnet and Killmilk have been seen selling logs, data, and accesses on their Telegram channels and the Infinity forum since at least November 2022. These sales often relate to attacks that appear to be in line with their hacktivist activities, indicating that they are seizing the opportunity to monetize their actions. The authenticity of the data Killnet claims to be selling is unknown. Moreover, in most cases, it is not known whether the goods were actually sold. The high prices demanded are likely to reduce the likelihood of sales, as some actors have commented on their expensiveness. Below are some examples of the goods offered for sale.

Logs

In January 2023, Killmilk advertised the sale of logs from various countries including the US, Ukraine, and European countries. They claimed that this amounted to 150 million passwords and other types of data. The logs were offered for sale for 10 BTC.



Killmilk выставил на продажу 150 млн паролей жителей Европы, Америки, Украины и других недружественных стран: https://infinity.ink/threads/prodam-zhirnye-logi.189/

В данные входят:
- пароли от лк кабинетов банков
- данные кредитных и дебетовых карт
- крипто логи
- системы доступа к рабочим столам 6000 разных организаций со всего мира.
- gov порталы
И тысячи других доступов

Новый год дарит не только положительные эмоции, но и новую эскалацию по всему миру от KILLNET❤️

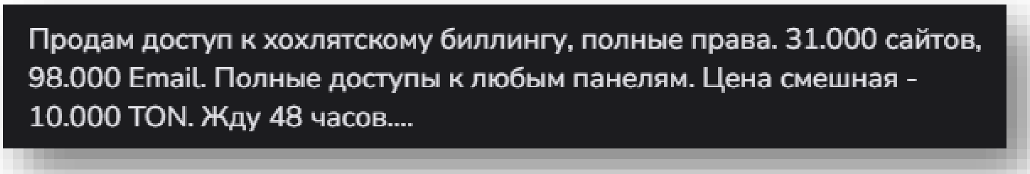
Post on Killnet's Telegram channel advertising 150 million passwords that Killmilk put up for sale on Infinity

Data

In March 2023, Killnet claimed to have hacked Rheinmetall, an arms manufacturing company. They stated that they would sell data on Rheinmetall employees for 5 BTC.

Accesses

- On January 16, 2023, Killmilk advertised the sale of access to a network of 6 restaurants, from a US food chain, for 1 BTC on the Infinity forum. There is no indication that the access was sold, with several actors complaining about the high price.
- On January 2, 2023, Killmilk announced on the Infinity forum the sale of 18 hacked email addresses of the Indian Ministry of Finance. They noted that the mailboxes contained more than a million documents and correspondence. They offered access to the mailboxes for 15 BTC.
- On December 22, 2022, access to a Ukrainian billing provider was advertised for sale, for 10,000 TON, on the Killnet and Killmilk Telegram channels. It is claimed that the access included full rights, with access to 31,000 sites and 98,000 emails. It appears Killmilk attempted to monetize this access again in January 2023 when they advertised the sale of 50,000 logs, including access to corporate emails, database servers, Cpanel panels, and more, this time significantly more expensive - for 30 BTC on the Infinity forum. The screenshots posted as proof hinted the information was extracted from the aforementioned billing provider.



Продам доступ к хохлятскому биллингу, полные права. 31.000 сайтов, 98.000 Email. Полные доступы к любым панелям. Цена смешная - 10.000 TON. Жду 48 часов....

Access to a Ukrainian billing provider advertised for sale

Ransoms

In several instances, Killnet has attempted to extort victims into paying a ransom by either threatening to release stolen data or to continue conducting DDoS attacks. They have used this method when attacking organizations, as well as cybercrime marketplaces and forums. In one instance, they claimed to have successfully collected a ransom from their victim.

RuTor

On August 15, 2022, Killnet announced the start of a DDoS campaign targeting RuTor, a cybercrime forum, claiming that the forum is owned by the Security Service of Ukraine. On August 19, 2022, Killmilk announced on their Telegram channel that they had received a payment of USD 15,000 from RuTor in exchange for stopping attacks. Despite Killnet's claims, there is evidence suggesting that the site remained accessible for at least some of the period that Killnet were conducting attacks.

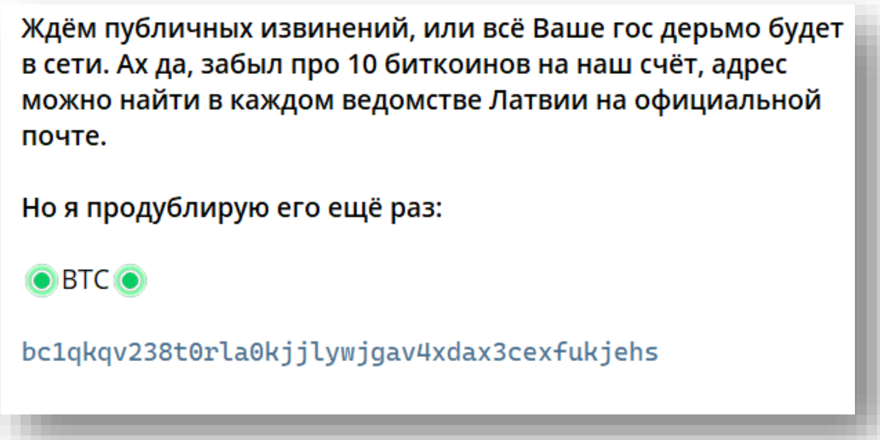
BlackSprut

On November 28, 2022, Killnet and Deanon Club announced that they had DDosed BlackSprut, a drug market, and had stolen various types of data. BlackSprut were given 24 hours to get in contact and to negotiate.

A day later, likely after no ransom was paid, Killmilk announced the sale of the data, splitting it into parts priced between USD 3000 and USD 1 million. The data included a database and the identity of the owner of BlackSprut and his "madam". It appears as though at least some of this data had not been sold as it was advertised again by Deanon Club in February-March 2023.

Latvian Government

In November 2022 Killnet claimed to have compromised the email account of an employee from the Latvian State Revenue Service. They noted that they were able to get access to the corporate network, including VPN and 200GB of data they were able to download. They shared proof of their access and demanded 10 BTC from Latvia, giving them 10 hours to pay. After no ransom payment was made, on December 1, 2022, Killnet announced that they would sell the data for 1 BTC.



Ждём публичных извинений, или всё Ваше гос дерьмо будет в сети. Ах да, забыл про 10 биткоинов на наш счёт, адрес можно найти в каждом ведомстве Латвии на официальной почте.

Но я продублирую его ещё раз:

🟢BTC🟢

bc1qkqv238t0rla0kjjlywjgav4xdax3cexfukjehs

Killnet demands 10 BTC in ransom from Latvian Government

NATO

On April 13, 2023, Killmilk claimed to have hacked the NATO Learning Management System. They claimed to have stolen various types of data, including documents on private military methodology and students. A ransom of 3 BTC was demanded from NATO, warning NATO members “Pay me and I will be silent”. Later on the same day, they also claimed to have hacked the NATO Communications and Information Agency, possibly a part of the same attack.

On April 17, 2023, Killmilk announced that NATO had not paid for their data, which they claimed included data from the E-portal. They advertised the sale of logs priced at USD 1 per log. Sample files and screenshots of the data were shared on the Telegram channel.

Infinity forum

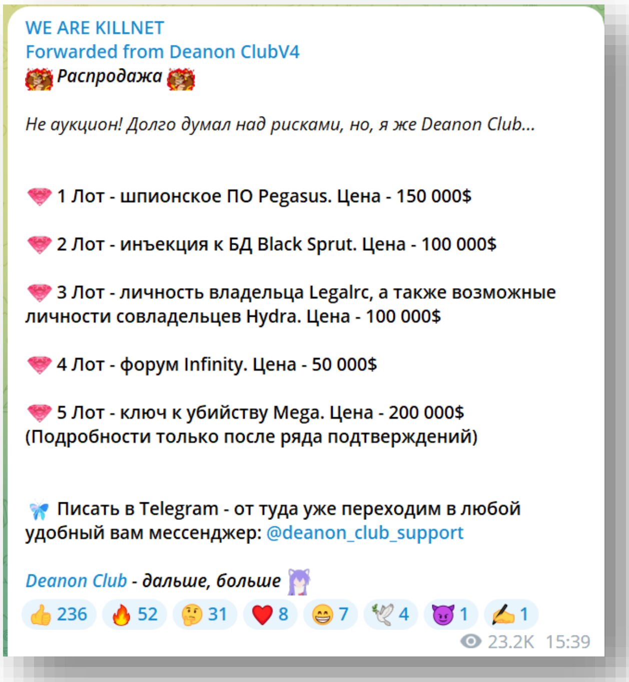
At the end of November 2022, Killnet and Deanon Club announced a joint project - a hacking forum called Infinity. First, a Telegram chat was started for the forum and the forum was later launched on December 31, 2022.

The forum presented Killnet with new income sources[4]:

- Advertising: The advertisement packages on the Infinity forum reportedly included main-page banner advertisements for USD 250-1,000 per month, depending on their size, as well as other paid ads options. KELA has observed different ads on the forum, suggesting there were users paying for the service.
- Statuses: Four levels of statuses on the forum were available for purchase: "Kommersant" sold at USD 299; "Businessman" sold at USD 599; "God of the market" sold at USD 999; and, "Exchange office" sold at USD 1499 per month and required a 0.5 BTC deposit.

Despite the forum being promoted across Killnet's Telegram channels, and other Russian hacktivist groups' Telegram channels, Infinity never became a popular forum in comparison to other known Russian language forums. On February 19, 2023, Killmilk announced that they were selling Infinity, possibly prompted by the lack of growth of the forum. On March 11, 2023, the sale was temporarily suspended, however, it resumed on Deanon Club's Telegram channel for USD 50,000 on March 31. On April 12, Killmilk reduced the price of the Infinity forum to USD 25,000.

[4] Radware



WE ARE KILLNET
Forwarded from Deanon ClubV4

🎁 *Распродажа* 🎁

Не аукцион! Долго думал над рисками, но, я же Deanon Club...

💎 1 Лот - шпионское ПО Pegasus. Цена - 150 000$

💎 2 Лот - инъекция к БД Black Sprut. Цена - 100 000$

💎 3 Лот - личность владельца Legalrc, а также возможные личности совладельцев Hydra. Цена - 100 000$

💎 4 Лот - форум Infinity. Цена - 50 000$

💎 5 Лот - ключ к убийству Mega. Цена - 200 000$
(Подробности только после ряда подтверждений)

🎀 Писать в Telegram - от туда уже переходим в любой удобный вам мессенджер: @deanon_club_support

Deanon Club - дальше, больше

👍 236 🔥 52 🤔 31 ❤️ 8 😁 7 🕊 4 😈 1 ✍ 1
23.2K 15:39

Deanon Club Telegram post advertising the sale of various lots including Infinity forum for USD 50,000

There is no indication that the forum was successfully sold. At the end of May 2023, Infinity forum's domain was repurposed to advertise Tesla-Botnet, a botnet developed by Radis, the leader of Anonymous Russia.

While Killnet has tried different methods to earn funds, it appears none of the methods seemed to be sufficient enough to be chosen as a dominant one; it is, therefore, possible that Killnet's attempts will continue, resulting in more efforts to monetize their hacktivist attacks and/or create new products for the cybercrime ecosystem.

Anonymous Russia

Anonymous Russia is a pro-Russian hacktivist group that has conducted attacks, primarily DDoS, against Ukraine and its supporters, including Poland, Germany, the UK, Armenia, the Czech Republic, Slovakia, and Estonia. In April 2023, 'Radis' was made leader of the group after the previous leader 'Raty' was arrested.[5] After Radis' takeover of Anonymous Russia, the group moved away from asking for donations from their supporters and instead, launched several paid-for services/products, most notably Tesla-Botnet, a botnet[6] developed by Radis, which has been advertised on Anonymous Russia's Telegram channel.

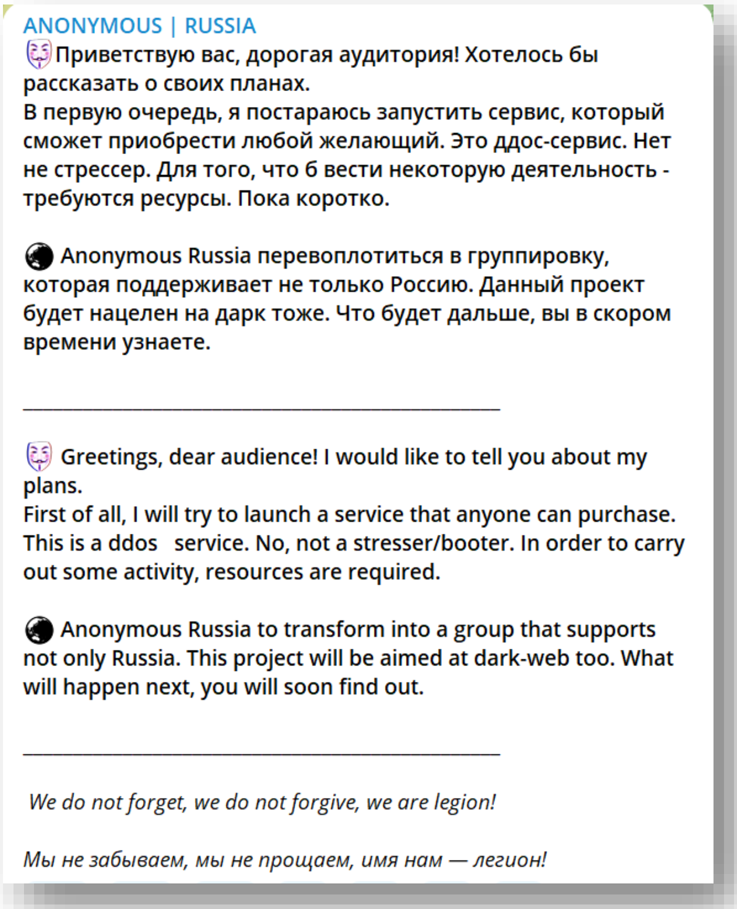
Tesla-Botnet

In April 2023, Tesla-Botnet was announced, with the release set for April 28, 2023. Three different tariffs are available for sale: Basic, Pro, and Rare (USD 50, USD 120, and USD 220 respectively) based on the number of bots the clients want to use in attacks. Basic provides its users with ten bots whilst Rare provides them with 50. The Tesla-Botnet Telegram channel has over 1000 subscribers.

DDoS TOR service

After taking control of Anonymous Russia in April 2023, Radis announced their plans to develop a DDoS service that anyone can purchase. They stated that the project would also be aimed at the dark web suggesting that Anonymous Russia will target underground markets, something Killnet has also been observed doing.

[5] Новая газета Европа.
[6] A botnet is a network of compromised devices infected by malware which are under the control of an attacker. Each compromised device is referred to as a bot.



ANONYMOUS | RUSSIA

Приветствую вас, дорогая аудитория! Хотелось бы рассказать о своих планах.
В первую очередь, я постараюсь запустить сервис, который сможет приобрести любой желающий. Это ддос-сервис. Нет не стрессер. Для того, что б вести некоторую деятельность - требуются ресурсы. Пока коротко.

Anonymous Russia перевоплотиться в группировку, которая поддерживает не только Россию. Данный проект будет нацелен на дарк тоже. Что будет дальше, вы в скором времени узнаете.

Greetings, dear audience! I would like to tell you about my plans.
First of all, I will try to launch a service that anyone can purchase. This is a ddos service. No, not a stresser/booter. In order to carry out some activity, resources are required.

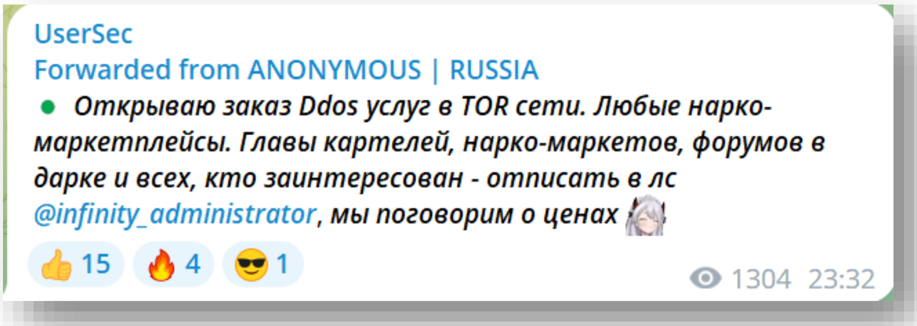
Anonymous Russia to transform into a group that supports not only Russia. This project will be aimed at dark-web too. What will happen next, you will soon find out.

We do not forget, we do not forgive, we are legion!

Мы не забываем, мы не прощаем, имя нам — легион!

Announcement of an upcoming DDoS service by Anonymous Russia in April 2023

On May 4, 2023, Anonymous Russia announced the launching of a DDoS service targeting Tor sites. The post has since been deleted from the channel and it is unclear if the service is still available.



UserSec
Forwarded from ANONYMOUS | RUSSIA

● ***Открываю заказ Ddos услуг в TOR сети. Любые нарко-маркетплейсы. Главы картелей, нарко-маркетов, форумов в дарке и всех, кто заинтересован - отписать в лс @infinity_administrator, мы поговорим о ценах***

Anonymous Russia's announcement of a new DDoS service. The post was forwarded to the UserSec Telegram channel

Radis announced on May 15, 2023, that they will be engaging in commercial activities and will no longer be accepting donations. They stated that the money earned will be used to attack Ukrainian network infrastructure. They noted their plans to create a trusted sellers board where verified sellers will be listed, as well as to partner with Deanon Club and Titan Stealer, an information stealer operation.

The Anonymous Russia Telegram channel was not active throughout June. In July, the group re-emerged, declaring a new leader - ‘User1’, the founder of another pro-Russian group, UserSec. It remains to be seen how the change in leadership will affect Anonymous Russia’s monetization attempts.

Phoenix

Phoenix is a pro-Russian hacktivist group that initially was a sub-team of Legion (a pro-Russian hacktivist collective established by Killnet in April 2022 to conduct DDoS attacks) but has since become its own entity, operating its own Telegram channel where it posts about its activities. Phoenix primarily conducts DDoS attacks but also has conducted website defacements, as well as leaking stolen data and sharing compromised credentials to their Telegram channel.

Countries that have been targeted by Phoenix include Ukraine, the UK, the US, India, Pakistan, and Japan. Like other groups, Phoenix asks its supporters for donations on its Telegram channel to help fund its activities. However, beyond donations, Phoenix has been observed using various other methods to source income, as described below. The leader of Phoenix stated in an interview that the salary earned from their activities is constantly fluctuating, noting that some months they can pay a salary of a hundred thousand rubles to senior "officers" and the next month they have to return to their day job to pay off loans.[7]

Selling of stolen data

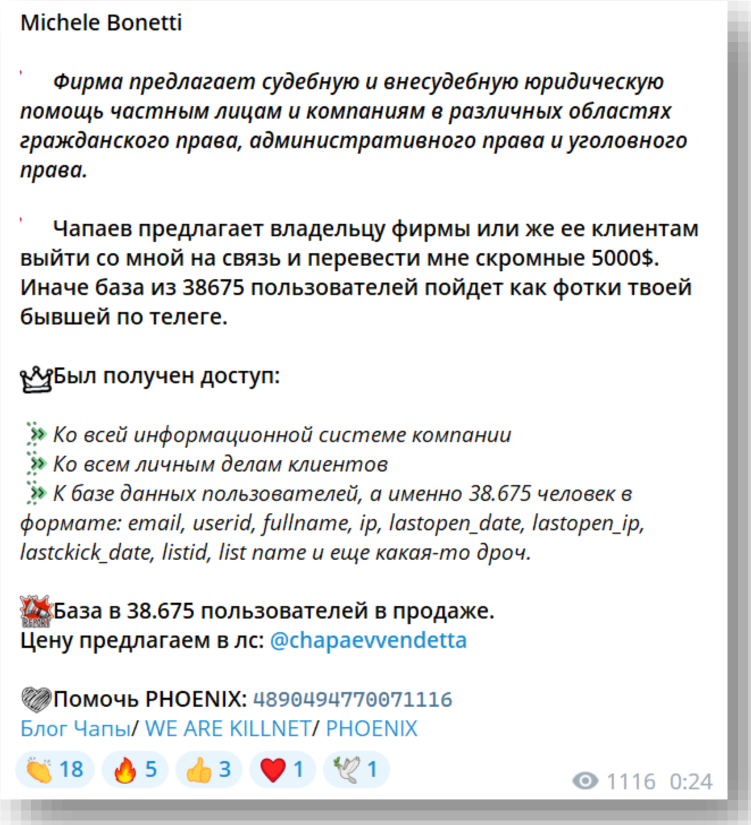
In several instances Phoenix has been observed selling allegedly stolen data on their Telegram channel. In addition, they have a separate channel called "Phoenix Shop", created in March 2023, which they stated would sell the "results of the work of the Phoenix group". However, this channel does not have many subscribers and is not currently active.

Ransoms

In addition to selling stolen data to interested parties, Phoenix has also been seen on several occasions using this data to try and extort their victims into paying a ransom.

On April 15, 2023, Phoenix claimed to have attacked the law firm, Michele Bonetti. They stated that they obtained a database containing information on over 38,000 users. Chapaev (Чапаев), the leader of Phoenix, instructed Michele Bonetti and/or their clients to contact them and pay a ransom of USD 5,000.

[7] Gazeta.ru



Michele Bonetti

Фирма предлагает судебную и внесудебную юридическую помощь частным лицам и компаниям в различных областях гражданского права, административного права и уголовного права.

Чапаев предлагает владельцу фирмы или же ее клиентам выйти со мной на связь и перевести мне скромные 5000$. Иначе база из 38675 пользователей пойдет как фотки твоей бывшей по телеге.

Был получен доступ:

» Ко всей информационной системе компании
» Ко всем личным делам клиентов
» К базе данных пользователей, а именно 38.675 человек в формате: email, userid, fullname, ip, lastopen_date, lastopen_ip, lastckick_date, listid, list name и еще какая-то дроч.

База в 38.675 пользователей в продаже.
Цену предлагаем в лс: @chapaevvendetta

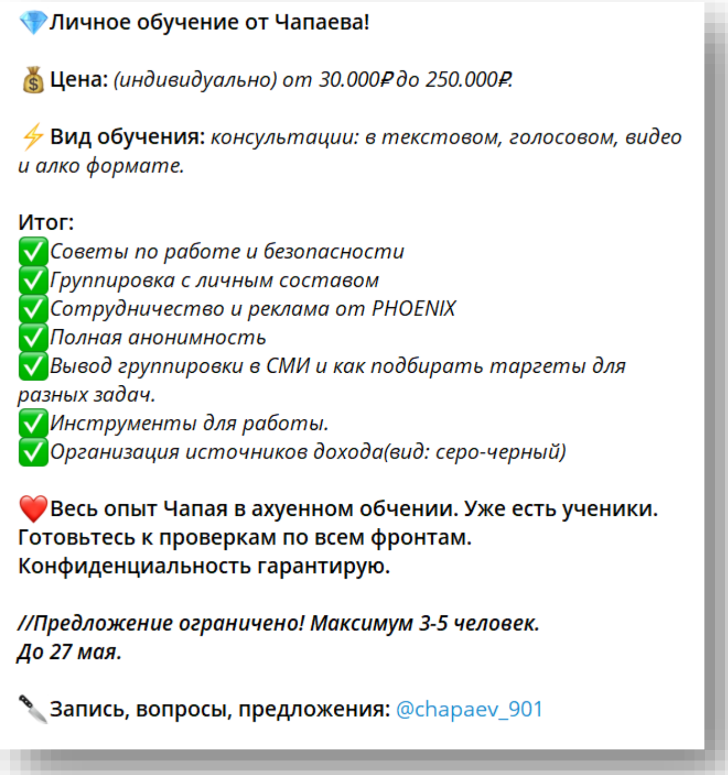
Помочь PHOENIX: 4890494770071116
Блог Чапы/ WE ARE KILLNET/ PHOENIX

Phoenix demands USD 5,000 ransom for the stolen database

Separately, on March 29, 2023, Phoenix claimed to have attacked Cellular Pacific and to have gained access to various types of data within the network, including customer orders, sales reports, and a list of clients. They released screenshots of some of the stolen data and instructed Cellular Pacific to get in touch. No additional information on a ransom is mentioned, but it is likely that Phoenix were looking to extort a ransom payment from Cellular Pacific in return for not publishing or selling the data.

Selling training

On May 16, 2023, Phoenix announced on their Telegram channel that they were offering personal training from their leader, Chapaev, for 30,000-250,000 rubles. The offer was available until May 27 and there were only up to five places available.



💎**Личное обучение от Чапаева!**

💰**Цена:** *(индивидуально) от 30.000₽ до 250.000₽.*

⚡**Вид обучения:** *консультации: в текстовом, голосовом, видео и алко формате.*

Итог:
✅*Советы по работе и безопасности*
✅*Группировка с личным составом*
✅*Сотрудничество и реклама от PHOENIX*
✅*Полная анонимность*
✅*Вывод группировки в СМИ и как подбирать таргеты для разных задач.*
✅*Инструменты для работы.*
✅*Организация источников дохода(вид: серо-черный)*

❤️**Весь опыт Чапая в ахуенном обчении. Уже есть ученики. Готовьтесь к проверкам по всем фронтам. Конфиденциальность гарантирую.**

//Предложение ограничено! Максимум 3-5 человек. До 27 мая.

🔪**Запись, вопросы, предложения:** @chapaev_901

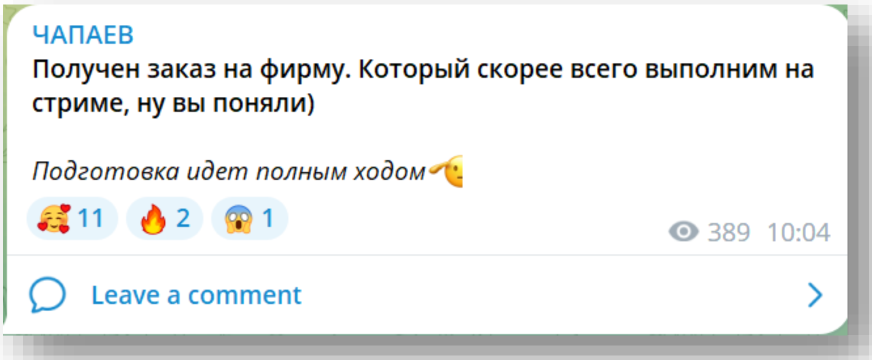
Phoenix announces private training courses

Previously, on April 11, 2023, personal consultations with Chapaev were advertised on the Phoenix Telegram channel. No price was set with it stating that the price was negotiable. The advertised content of these consultations was extremely broad, with the post stating that Chapaev will tell his students how to hack an ex, how to live and listen to "all your nonsense." In a follow-up to this post, it was announced that anyone who donated 1000 rubles wold be able to talk with Chapaev over the phone, and anyone who donated 5000 rubles would be able to video call. Individuals that donated over USD 100 would be allowed to conduct attacks with Chapaev.

DDoS-for-hire services

In an interview with Gazeta.ru, published in February 2023, Chapaev stated that one of their sources of income is through DDoS-for-hire services. For instance, they noted that they had received orders from organizations or individuals in Italy and Spain to DDoS the countries' government websites (Chapaev assumed the order was coming from political opposition in these countries). In the interview, they also state that a source of income is through hacking cryptocurrency-related services.[8]

A post on Chapaev's Telegram channel from May 5, 2023, suggests that they are still taking orders, with the post stating that "an order has been received" and that the attack will be done over a live stream (see section 'Streaming attacks'). However, seeing as these services are not actively promoted on their channel, it does not appear as though this is a focus for the group.



ЧАПАЕВ

Получен заказ на фирму. Который скорее всего выполним на стриме, ну вы поняли)

Подготовка идет полным ходом🫡

Chapaev announces that they have received an order for an attack

[8] Gazeta.ru

Streaming attacks

In April 2023, Phoenix announced that they would begin video and audio streaming their attacks, stating that this coverage will increase the coverage of Phoenix in the media and will result in an influx of funds “that will be converted into medicines, drones, and other humanitarian value” that is needed for Russian soldiers. Phoenix appears to have used both Telegram and YouTube for their streams. In addition to counting on additional donations as a result of the streams, Phoenix also introduced other means of earning income through the stream:

- On May 11, 2023, an auction was announced in which the highest bidder would get to appear on the stream
- They stated that they would welcome sponsors for the stream
- Interested parties can buy advertising for the streams

The approach is quite unique and, as opposed to other means, is focused on increasing the number of donations rather than relying only on additional income sources. In addition to acting as a funding source for their own operations, a proportion of the money earned through the auction and streams is donated to the Russian Army according to Phoenix.

Anonymous Sudan

Anonymous Sudan, a relatively new group compared to the groups discussed above, is a hacktivist group that emerged in January 2023, with the purpose of “proving to all countries that Sudan has people who will protect it on the Internet” and to “attack anyone who opposes Islam”.

The group, which is not affiliated to the wider Anonymous collective, is believed by some researchers to be linked to Russia with some stating that they are another Russian hacktivist group, whilst others assess that the group is possibly connected to the Russian state. The group is not believed to be affiliated with the *original* Anonymous Sudan group that emerged in 2019. [9]

On February 19, 2023, Anonymous Sudan announced that going forward they will be an official member of Killnet. Anonymous Sudan has emphasized that they are not a Russian group but partnered with Killnet and supported Russia in return for the help they received from Killnet, in addition to Russia’s previous support of Sudan.

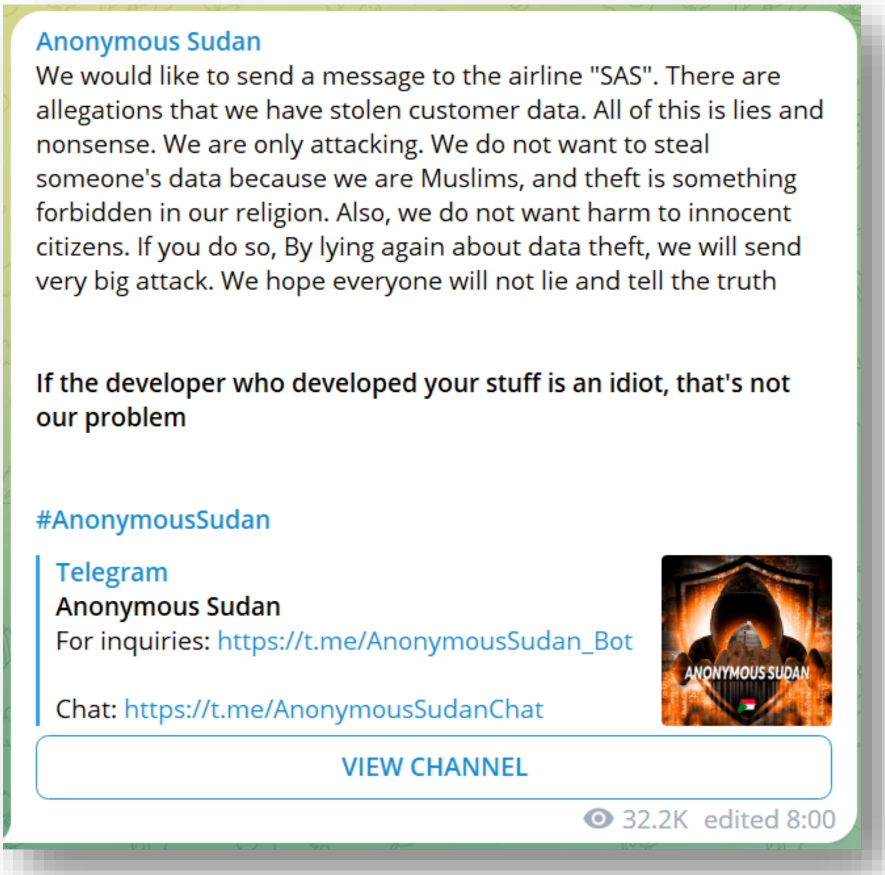
Anonymous Sudan has targeted organizations from various countries including Sweden, the Netherlands, Germany, Denmark, Spain, the US, Poland, France, Australia, Israel, India, Ethiopia, and the UAE. These attacks are often either in support of Killnet or in response to anti-Muslim events taking place in these countries.

Beyond donations, Anonymous Sudan’s efforts to monetize their operations are isolated to selling stolen data or demanding a ransom from their victims in exchange for ending DDoS attacks. At this point, there are only a few examples of such behavior, indicating that income generation is not the primary focus.

[9] Truesec; CyberCX; Trustwave

Selling of stolen data

In 2023, Anonymous Sudan were observed selling stolen data in several instances marking a significant departure from their initial modus operandi as they had previously stated that they would not steal data as this is "forbidden in their religion".



Anonymous Sudan

We would like to send a message to the airline "SAS". There are allegations that we have stolen customer data. All of this is lies and nonsense. We are only attacking. We do not want to steal someone's data because we are Muslims, and theft is something forbidden in our religion. Also, we do not want harm to innocent citizens. If you do so, By lying again about data theft, we will send very big attack. We hope everyone will not lie and tell the truth

If the developer who developed your stuff is an idiot, that's not our problem

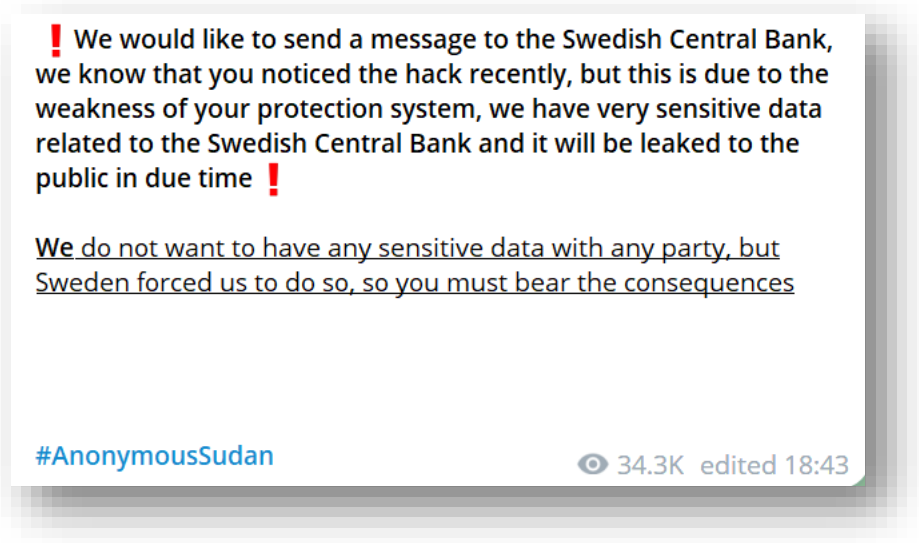
#AnonymousSudan

Telegram
Anonymous Sudan
For inquiries: https://t.me/AnonymousSudan_Bot

Chat: https://t.me/AnonymousSudanChat

Figure 4: Anonymous Sudan denies stealing data in February 2023

Despite this claim, less than a month later the group had begun threatening to leak stolen data. While some of the data was initially released for free, there were multiple instances where Anonymous Sudan attempted to sell data from an attack on their Telegram channel.



❗ We would like to send a message to the Swedish Central Bank, we know that you noticed the hack recently, but this is due to the weakness of your protection system, we have very sensitive data related to the Swedish Central Bank and it will be leaked to the public in due time ❗

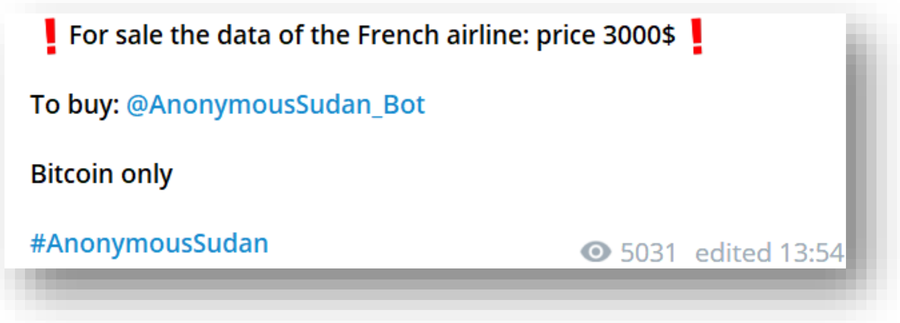
We do not want to have any sensitive data with any party, but Sweden forced us to do so, so you must bear the consequences

#AnonymousSudan

👁 34.3K edited 18:43

Figure 5: Anonymous Sudan announces that they will release data from the Swedish Central Bank

On March 19, 2023, Anonymous Sudan claimed to have attacked Air France and to have stolen data. A proof of data was released, which based on KELA's review appears to be customer credentials, consisting of either an email address or a string of numbers (possibly a Flying Blue number), and a password. Only twelve credentials were shared in the sample data. These credentials are likely used to access the customer portal. The group advertised the sale of the data belonging to Air France for USD 3000.



❗ For sale the data of the French airline: price 3000$ ❗

To buy: @AnonymousSudan_Bot

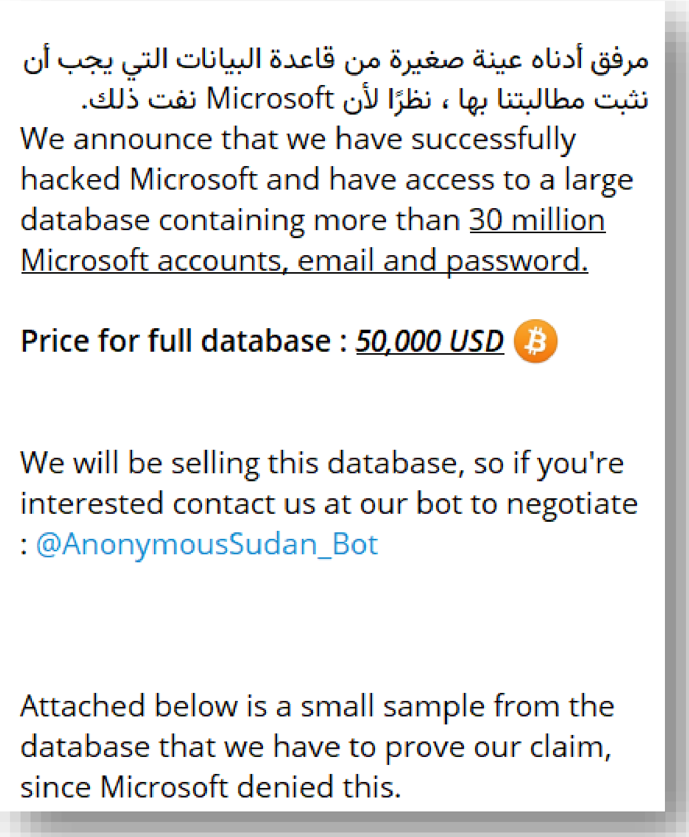
Bitcoin only

#AnonymousSudan

👁 5031 edited 13:54

Figure 6: Anonymous Sudan advertises the sale of Air France data

Furthermore, on July 2, 2023, Anonymous Sudan announced that they had hacked Microsoft and claimed to have gained access to a database containing more than 30 million Microsoft accounts (emails and passwords). They advertised the sale of this database for USD 50,000. Anonymous Sudan first claimed to have obtained data from Microsoft on June 6, 2023, during the series of DDoS attacks they launched against Microsoft (see section Ransom DDoS attacks). Microsoft has denied that data was stolen.[10]



مرفق أدناه عينة صغيرة من قاعدة البيانات التي يجب أن
نثبت مطالبتنا بها ، نظرًا لأن Microsoft نفت ذلك.

We announce that we have successfully hacked Microsoft and have access to a large database containing more than 30 million Microsoft accounts, email and password.

Price for full database : *50,000 USD* ₿

We will be selling this database, so if you're interested contact us at our bot to negotiate : @AnonymousSudan_Bot

Attached below is a small sample from the database that we have to prove our claim, since Microsoft denied this.

Anonymous Sudan announces they have stolen credentials for 30 million Microsoft accounts. They advertise the data for sale for USD 50,000

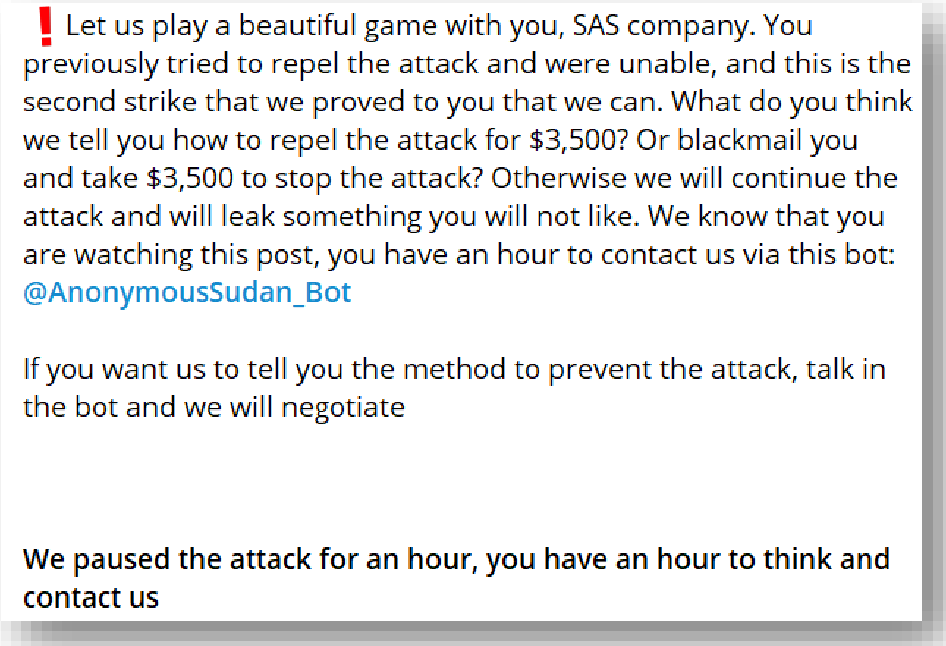
[10] Bleeping Computer

Ransom DDoS attacks

Since late May 2023, Anonymous Sudan were observed conducting several ransom DDoS attacks, including one targeting Scandinavian Airlines and another targeting Microsoft.

On May 24, 2023, Anonymous Sudan claimed to have attacked Scandinavian Airlines' (SAS) website and demanded a ransom of USD 3500 to stop the attack. On the same day, SAS customers complained about the app and website being down. SAS confirmed on May 24, 2023, that they were "experiencing technical issues with the website and app" although they did not confirm the reason why.[11]

After no ransom was paid, the group continued to target the airline, claiming on May 29, 2023, that the airline's services had been completely shut down for 5 days, while customers continued to complain. Anonymous Sudan has raised the ransom from USD 3500 multiple times, with the most recent price set at USD 10 million on June 2, 2023.



❗ Let us play a beautiful game with you, SAS company. You previously tried to repel the attack and were unable, and this is the second strike that we proved to you that we can. What do you think we tell you how to repel the attack for $3,500? Or blackmail you and take $3,500 to stop the attack? Otherwise we will continue the attack and will leak something you will not like. We know that you are watching this post, you have an hour to contact us via this bot: @AnonymousSudan_Bot

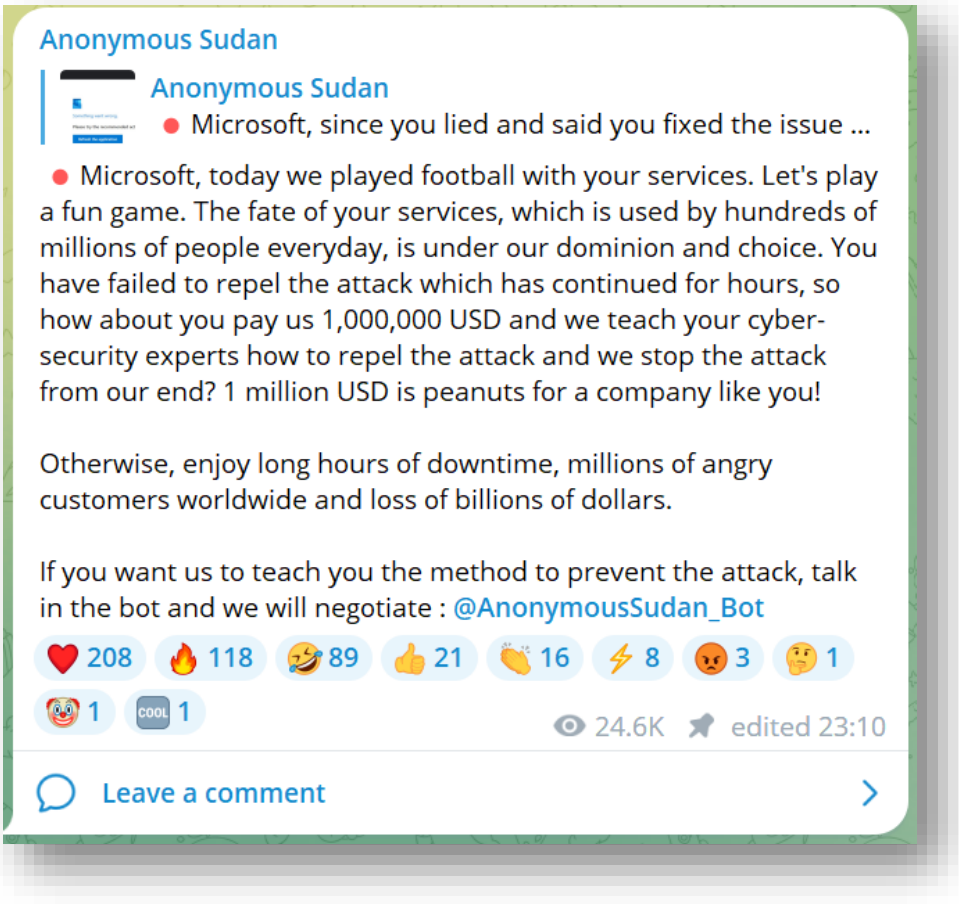
If you want us to tell you the method to prevent the attack, talk in the bot and we will negotiate

We paused the attack for an hour, you have an hour to think and contact us

Anonymous Sudan demands a ransom in exchange for stopping a DDoS attack

[11] Twitter

Furthermore, in addition to allegedly stealing data from Microsoft, from June 5, 2023, Anonymous Sudan claimed to have conducted DDoS attacks against several Microsoft services, including Outlook, SharePoint, OneNote, and Microsoft Teams. Microsoft stated that they were aware of issues accessing certain services.[12] They later confirmed that at the beginning of June, certain services had suffered availability issues as a result of a layer 7 DDoS attack, which Microsoft attributed to an actor it tracks as Storm-1359.[13] Anonymous Sudan demanded a USD 1 million ransom from Microsoft in order to stop the attacks.



Anonymous Sudan

Anonymous Sudan
● Microsoft, since you lied and said you fixed the issue ...

● Microsoft, today we played football with your services. Let's play a fun game. The fate of your services, which is used by hundreds of millions of people everyday, is under our dominion and choice. You have failed to repel the attack which has continued for hours, so how about you pay us 1,000,000 USD and we teach your cyber-security experts how to repel the attack and we stop the attack from our end? 1 million USD is peanuts for a company like you!

Otherwise, enjoy long hours of downtime, millions of angry customers worldwide and loss of billions of dollars.

If you want us to teach you the method to prevent the attack, talk in the bot and we will negotiate : @AnonymousSudan_Bot

Anonymous Sudan sets ransom for Microsoft

[12] Twitter
[13] Microsoft

Arvin Club

Arvin Club is a hacktivist group that is fighting against the Iranian government who they state are “killing my countrymen”.[14] The group has conducted DDoS attacks and hacked various Iranian organizations including the Ministry of Culture and Islamic Guidance.

The group maintains a Telegram channel, active since 2019, in which they post cybersecurity news, including news of recent breaches and ransomware strains. Links to leaked data and new ransomware blogs are commonly shared. In 2021-2022, the group maintained a free data leak site, which it seems to have re-established in July 2023. Most of the leaks posted by Arvin Club in the past were not unique or believed to have been sourced by them, but rather that Arvin Club was assembling public leaks.

Arvin Club has created two means of income on their Telegram channel, through the creation of a subscription-based channel, as well as by selling advertising spaces on their channel. Previously the group had sold data from their attacks, however, they stated in an interview that this is no longer a source of income for them.

Subscription-based Telegram channel

On April 29, 2023, Arvin Club announced a new private channel where “the latest news, exploits and vulnerabilities, as well as the latest links to ransomware and data leakage sites on the dark web” would be published. The channel is private and requires a subscription to access (USD 49 for lifetime access).

Advertising

Arvin Club allows for third-party advertising of goods and services on the Arvin Club Telegram channel. Interested parties are instructed to message the admin in Tox or Jabber for further information. It is highly likely that Arvin Club charges a fee for this advertising space.

[14] SuspectFile

Selling data

In an interview published in 2022, Arvin Club stated that they previously sold data from their attacks, or bought data and sold it as a middleman.[15] However, they noted that they have since stopped all these activities.[16]

Arvin now seems to be investing a lot more into building its brand within the cybersecurity ecosystem, rather than into hacktivist operations. With more than 4 years in action, this group may demonstrate a possible avenue for other, younger hacktivists groups. However, pro-Russian groups are yet to decide if they should follow this path or stick to their cause — if they are free to decide at all, considering their possible affiliation with the Russian government.

[15] SuspectFile.
[16] SuspectFile.

Other groups

In addition, there are several other hacktivist groups that have used some of the same methods as discussed above to earn some money and are worth mentioning.

Like Anonymous Russia, several pro-Russian groups have developed their own botnet. In addition to using these in their own attacks, they sell access to the botnet as well, for example, Passion, MistNet and NetSide.

Passion is a group that emerged in December 2022. It seems that from the beginning of their activities, the group used their own botnet to target Ukraine and its allies. Passion has been monetizing their operations since they emerged - two days after the channel was created, Passion botnet was offered for sale. Access to the botnet can be bought for varying time periods with the most recent prices in May 2023 starting at USD 30 per week. The owner of Passion botnet also announced a new botnet on March 18, 2023, called "GaechkaStress" which is available for sale for the same price. Passion was also observed selling other tools related to managing botnets. Like other groups, Passion has also tried to monetize their activities by demanding ransoms from their victims in exchange for stopping a DDoS attack.

As for the selling of data, there have been observations of other groups engaging in similar activities. The Islamic Cyber Corps is a hacktivist group acting in defense of Muslims, that has maintained a Telegram channel since April 2023. As part of their attacks, the group claims to steal data from numerous victims and threatens to sell this data on the dark web. The first instance of this occurred on April 17, 2023, and was followed by nine more occasions. KELA has not identified any evidence of this data being sold.

Some of these groups emerged more recently and, unlike some of the groups discussed in previous chapters, have looked to monetize their activities from the beginning.

Conclusion

Many active hacktivist groups emerged in the last year and a half. Donations are a method that a number of hacktivist groups have been observed using to help fund their activities. However, several groups have also looked for other means to source income. The success of these new practices is still yet to be determined. At least some of their methods do not appear to have been as successful as planned, for instance, Killnet's Infinity forum.

What this does show, is that these hacktivist groups do not intend to disappear - they are still committed to their cause. They are proactively looking for different ways that they can fund themselves. Their monetization efforts focus on selling data or demanding ransoms from their hacktivist campaigns, or looking for other sources of revenue from their supporters through the provision of training courses.

Although hack-for-hire services could possibly shift these groups away from hacktivism, and increase their threat, these services do not appear to be their focus. For instance, Killnet canceled its transition into a private military hacking company, and Phoenix, despite appearing to conduct DDoS-for-hire attacks, does not actively publicize this on their channel.

Therefore, the threat these groups pose and their dedication to hacktivism remains: they will continue to conduct DDoS attacks against organizations that they perceive have acted against their beliefs. In addition, these groups will likely continue to expand the types of attacks they conduct in an attempt to monetize their activities, either through the demanding of ransoms in DDoS attacks, or hacking into their victims' networks and claiming to have stolen data that they look to monetize (either through a ransom payment or through selling this data to interested parties).

In order to mitigate hacktivist activities, with DDoS staying their primary attack vector, it is recommended that organizations:

- **Monitor and filter traffic.** Monitor network traffic patterns and establish baselines to quickly identify abnormal or suspicious traffic that may indicate a DDoS attack, which can involve deploying network monitoring tools and anomaly detection systems. Implement traffic filtering mechanisms to block or limit traffic from suspicious sources or with characteristics indicative of DDoS attacks.

- **Monitor the cybercrime ecosystem.** Use a threat intelligence monitoring solution to continuously monitor for potential threats and take measures to prevent them. Such research should involve focused tracking of certain assets and specific threat actors, as well as broader monitoring of the latest trends, tools, and attack strategies discussed by cybercriminals.
- **Implement DDoS protection services and test public-facing systems.** Consider utilizing specialized DDoS protection solutions provided by reputable vendors, which protect public-facing systems against ongoing attacks, as well as proactively test them.
- **Create a DDoS response plan.** Developing a DDoS response plan is essential to effectively recognize threats and promptly restore operations after encountering DDoS attacks. This plan should include clear roles and responsibilities for the response team.
- **Educate employees on cybersecurity best practices.** Organizations should provide employees with annual cybersecurity training, including educating them about DDoS attacks, their impact, and the importance of reporting any suspicious activities.

Start monitoring the cybercrime underground for threats targeting your organization today - try KELA for free!