Dark Web Profile: Killnet – Russian Hacktivist Group

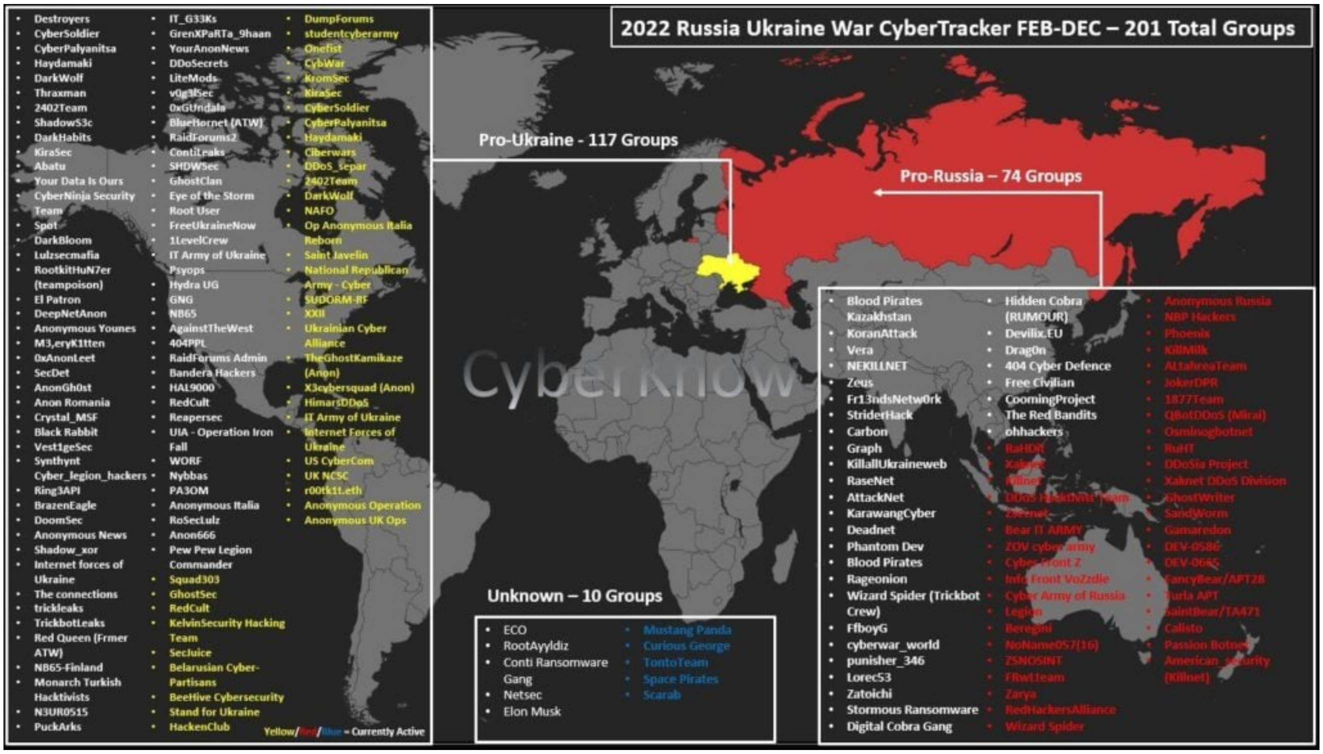
socradar.io/dark-web-profile-killnet-russian-hacktivist-group/

December 16, 2022

[Update] November 22, 2023: See the subheading: "Unrest Within KillNet: Internal Conflict and Public Criticism."

By SOCRadar Research

The ongoing conflict between Ukraine and Russia has attracted the attention of various cybercriminal groups and pushed them to get involved in this **cyber warfare**. According to CyberKnow's research, over 190 threat actor groups actively play a role during Ukraine-Russia cyber warfare.



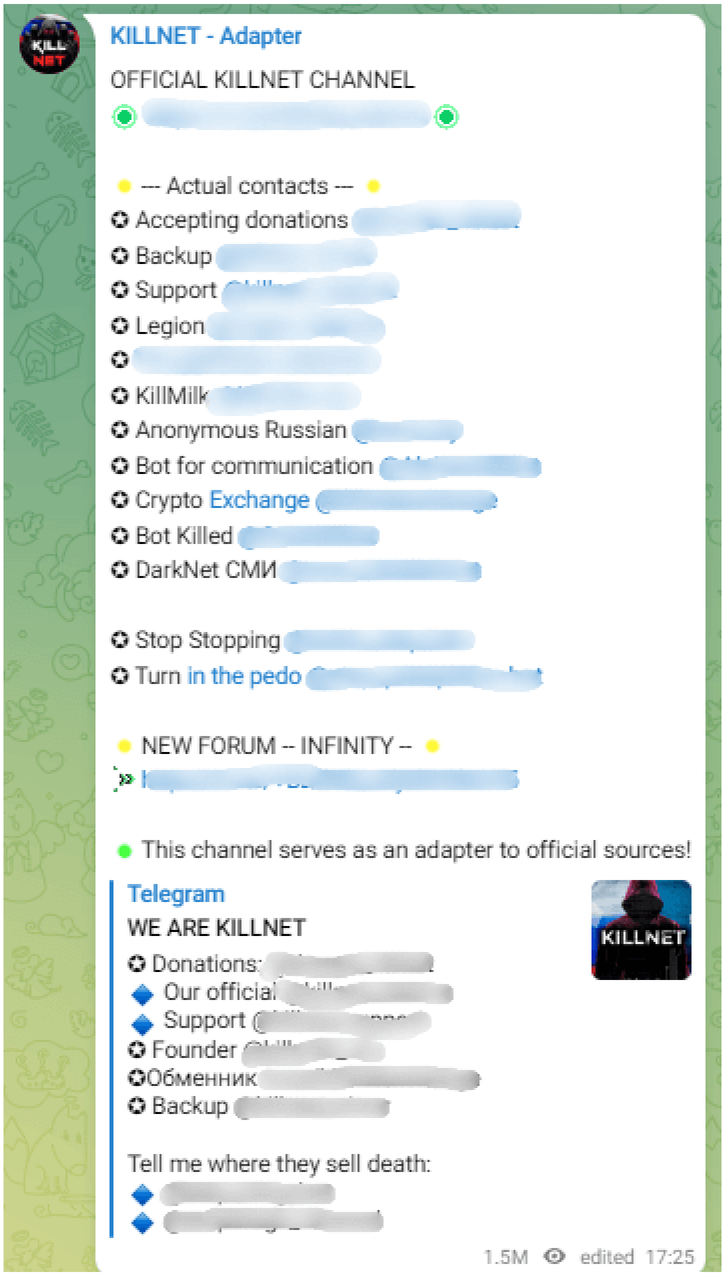
Some groups have aligned with one side of the conflict and are using their skills to support their chosen faction. KillNet is one of the groups that has played a significant role and is known for its **DDoS activities** in the interests of Russia.

Who is Killnet?

Killnet is a pro-Russian **hacktivist group** known for its DDoS campaigns against countries supporting Ukraine, especially NATO countries since the Russia-Ukraine war broke out last year. DDoS is the primary type of cyber-attack that can cause thousands of connection requests and packets to be sent to the target server or website per minute, slowing down or even stopping vulnerable systems.

While Killnet's **DDoS attacks** usually do not cause major damage, they can cause service outages lasting several hours or even days. It is known that **KillMilk**, its founder, left the group in July 2022, and its new leader is a hacker using the name **Blackside**. However, KillMilk is still related to the group and shares Killnet's announcements on his telegram channel, as seen below.

'OFFICIAL KILLNET CHANNEL' shared by Killnet in their Telegram group:



KILLNET - Adapter

OFFICIAL KILLNET CHANNEL

● [redacted] ●

● --- Actual contacts --- ●
✪ Accepting donations [redacted]
✪ Backup [redacted]
✪ Support [redacted]
✪ Legion [redacted]
✪ [redacted]
✪ KillMilk [redacted]
✪ Anonymous Russian [redacted]
✪ Bot for communication [redacted]
✪ Crypto Exchange [redacted]
✪ Bot Killed [redacted]
✪ DarkNet СМИ [redacted]

✪ Stop Stopping [redacted]
✪ Turn in the pedo [redacted]

● NEW FORUM -- INFINITY -- ●
» [redacted]

● This channel serves as an adapter to official sources!

> Telegram
> WE ARE KILLNET
> ✪ Donations: [redacted]
> 🔷 Our official [redacted]
> 🔷 Support [redacted]
> ✪ Founder [redacted]
> ✪Обменник [redacted]
> ✪ Backup [redacted]
>
> Tell me where they sell death:
> 🔷 [redacted]
> 🔷 [redacted]

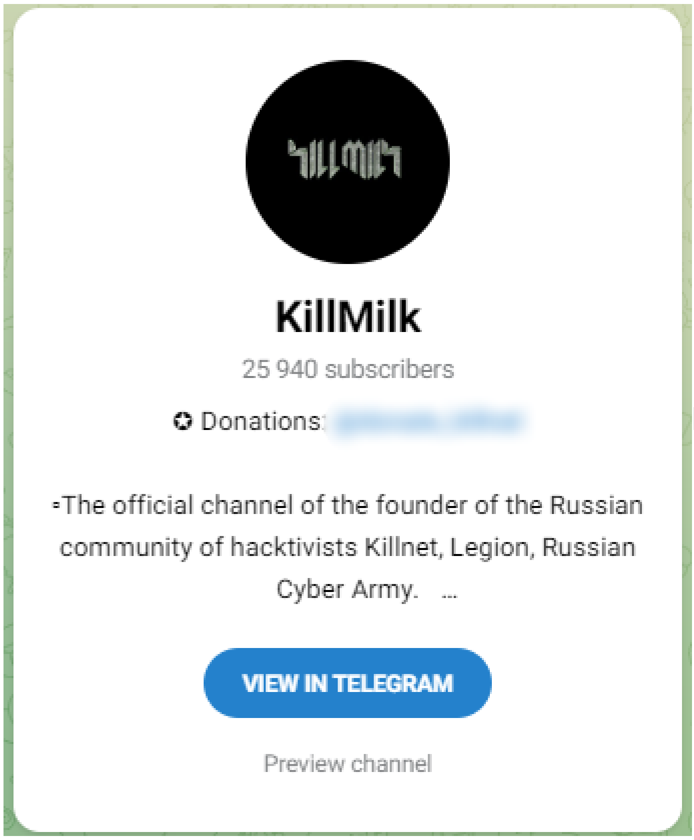
1.5M edited 17:25

Killnet Telegram Post

How Did Killnet DDoS Service Become a Hacktivist Group?

Until the Russia-Ukraine war, Killnet was known as the name of a DDoS attack tool that only subscribers could rent and use. With the crisis in Russia and Ukraine, Killnet emerged as a **hacker group** and continued its attacks under the name “Killnet.”
Afterward, the Killnet hacker group carried out many attacks to support Russia and fight for Russia’s interests. They targeted countries that supported **Ukraine** in the war between Russia and Ukraine. For months, the Killnet group has attacked the countries that support Ukraine, and their political interests are against the Russian government.

They do not seem interested in **financial gain**; they aim to harm web services by disrupting them with mainly DDoS attacks.



KillMilk

25 940 subscribers

✪ Donations: [redacted]

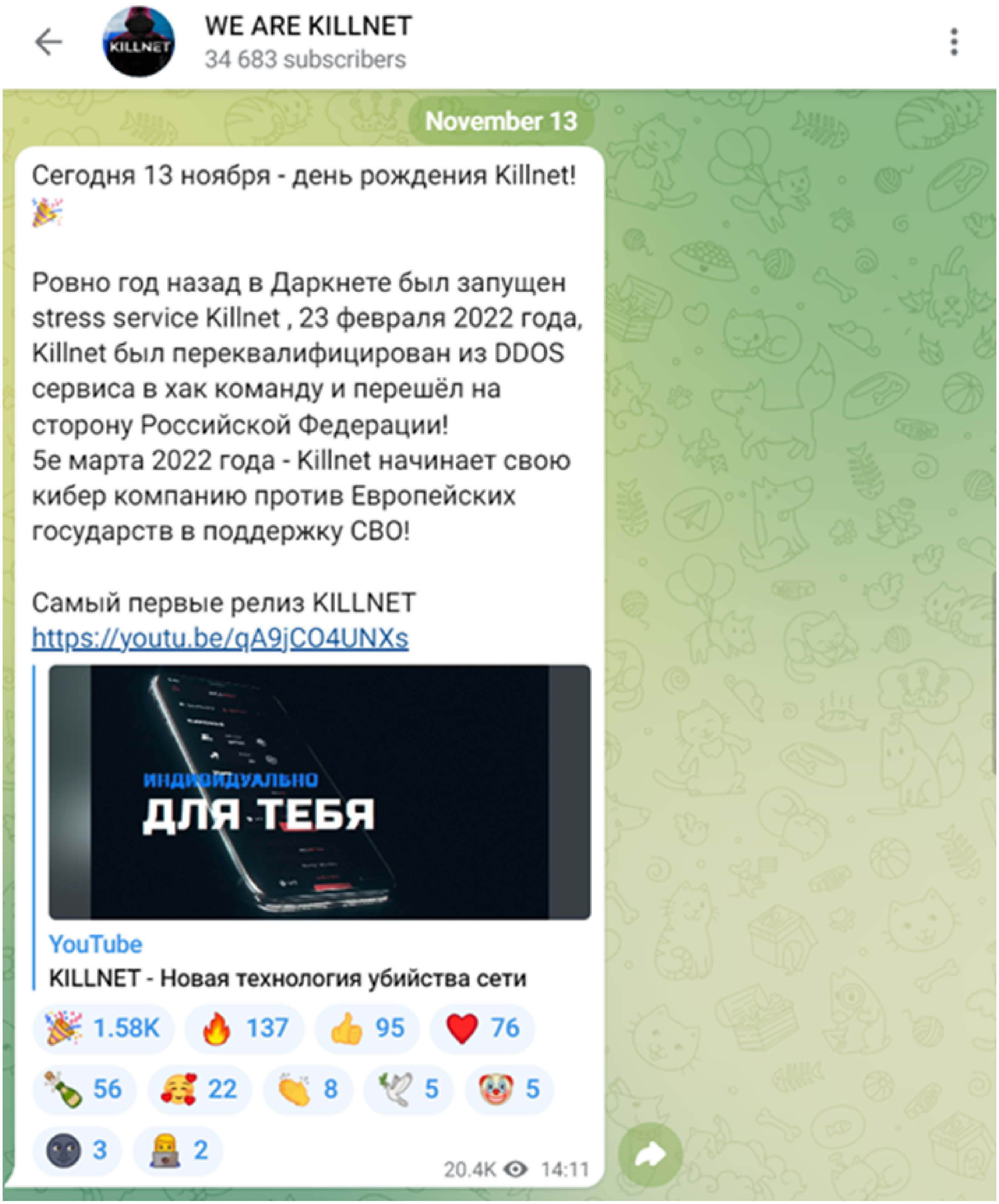
▪The official channel of the founder of the Russian community of hacktivists Killnet, Legion, Russian Cyber Army. ...

Figure 2: KillMilk Telegram Link

Killnet Grows

The group has continued its operations for over a year and has become a serious **cyber threat**. With the encouragement from Killnet service users, which reached tens of thousands of subscribers, they formed subgroups under the name “**Cyber Special Forces of the Russian Federation**.”

The group also started another hacker group called **LEGION** in April 2022 and continued its DDoS attacks from there. Other groups were observed under the LEGION group, each carrying out different attacks. In July 2022, the group announced that LEGION had been disbanded and would be relaunched as **LEGION 2.0**. There are more than a thousand estimated group members with all these related groups.



WE ARE KILLNET
34 683 subscribers

November 13

Сегодня 13 ноября - день рождения Killnet!
🎉

Ровно год назад в Даркнете был запущен stress service Killnet , 23 февраля 2022 года, Killnet был переквалифицирован из DDOS сервиса в хак команду и перешёл на сторону Российской Федерации!
5е марта 2022 года - Killnet начинает свою кибер компанию против Европейских государств в поддержку СВО!

Самый первые релиз KILLNET
https://youtu.be/qA9jCO4UNXs

YouTube
KILLNET - Новая технология убийства сети

🎉 1.58K 🔥 137 👍 95 ❤️ 76
🍾 56 🥰 22 👏 8 🕊 5 🤡 5
🌚 3 👨‍💻 2

20.4K 👁 14:11

Killnet mentioned in a post on their Telegram channel that their birth date is November 13, 2021. However, they announced that they became a hacktivist group on February 23, 2022.

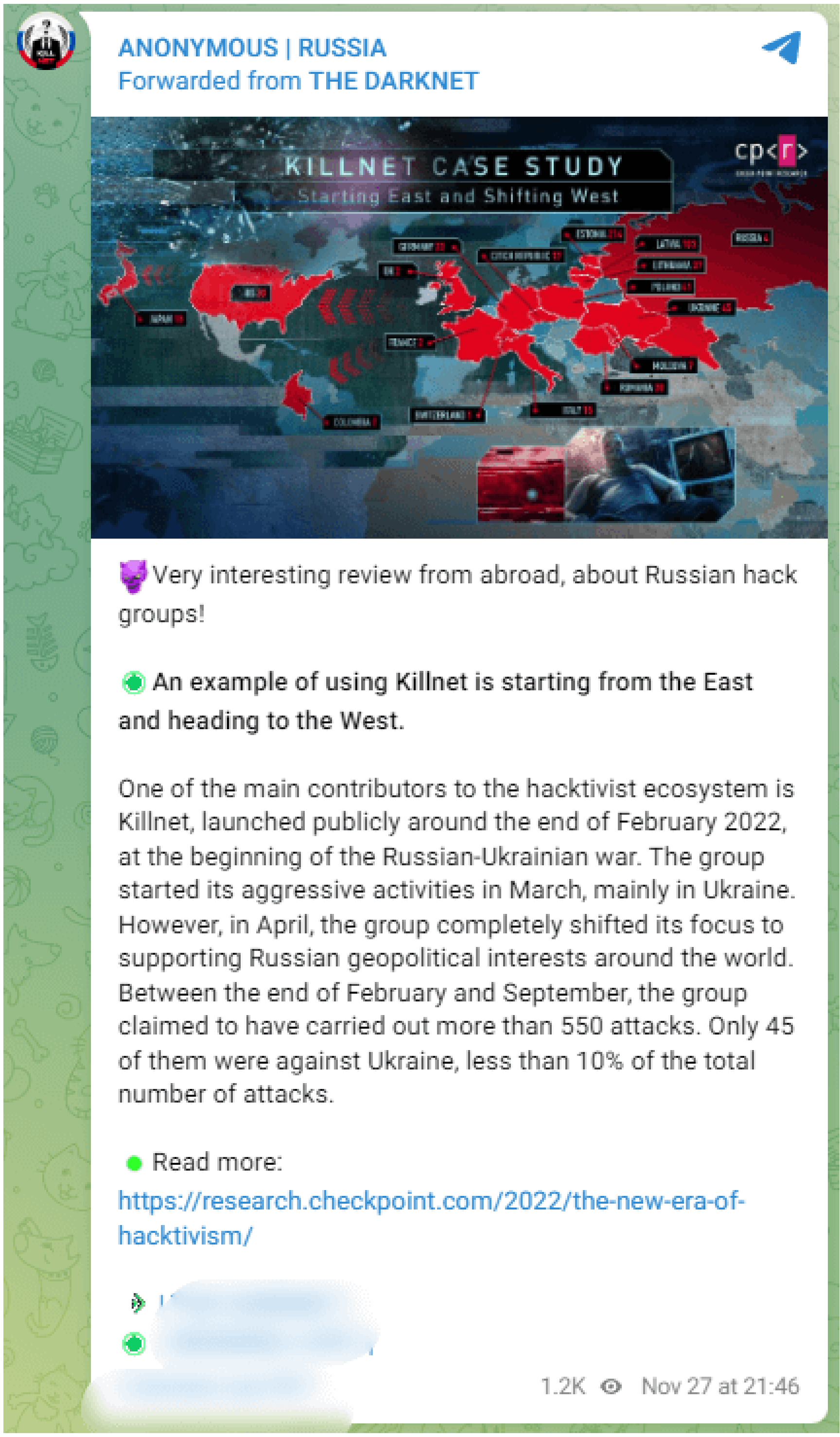
Killnet’s Relationship with Other Hacker Groups

A group formerly known as **XakNet** announced that it had merged with Killnet, targeting critical infrastructures. Another group, later known as **F**kNet**, also expressed its intention to work with Killnet, targeting the public and private sectors in countries that support Ukraine.

A former member of Killnet, now the leader of the **Zarya** group, also mentioned that other hacker groups act parallel with them and defend Russia's interests in an interview. He named groups like **XakNet**, **Beregini**, **CyberArmy**, **Anonymous Russia**, **RaHDit**, **DPR Joker**, **NoName057**, and **Zsecnet**.

The Hacker also said that Anonymous Russia and the Zarya group were founded by hackers who left the Killnet group. Other hackers also joined Zarya from Killnet.

In the same interview, Zarya's leader also explained the reasoning behind the creation of small groups by dividing Killnet. Smaller groups are easier to manage, and it is more difficult for the enemy to understand from whom to attack. He also revealed that Zarya was previously a part of the Killnet team but is now an independent entity.



ANONYMOUS | RUSSIA
Forwarded from THE DARKNET

😈Very interesting review from abroad, about Russian hack groups!

An example of using Killnet is starting from the East and heading to the West.

One of the main contributors to the hacktivist ecosystem is Killnet, launched publicly around the end of February 2022, at the beginning of the Russian-Ukrainian war. The group started its aggressive activities in March, mainly in Ukraine. However, in April, the group completely shifted its focus to supporting Russian geopolitical interests around the world. Between the end of February and September, the group claimed to have carried out more than 550 attacks. Only 45 of them were against Ukraine, less than 10% of the total number of attacks.

● Read more:
https://research.checkpoint.com/2022/the-new-era-of-hacktivism/

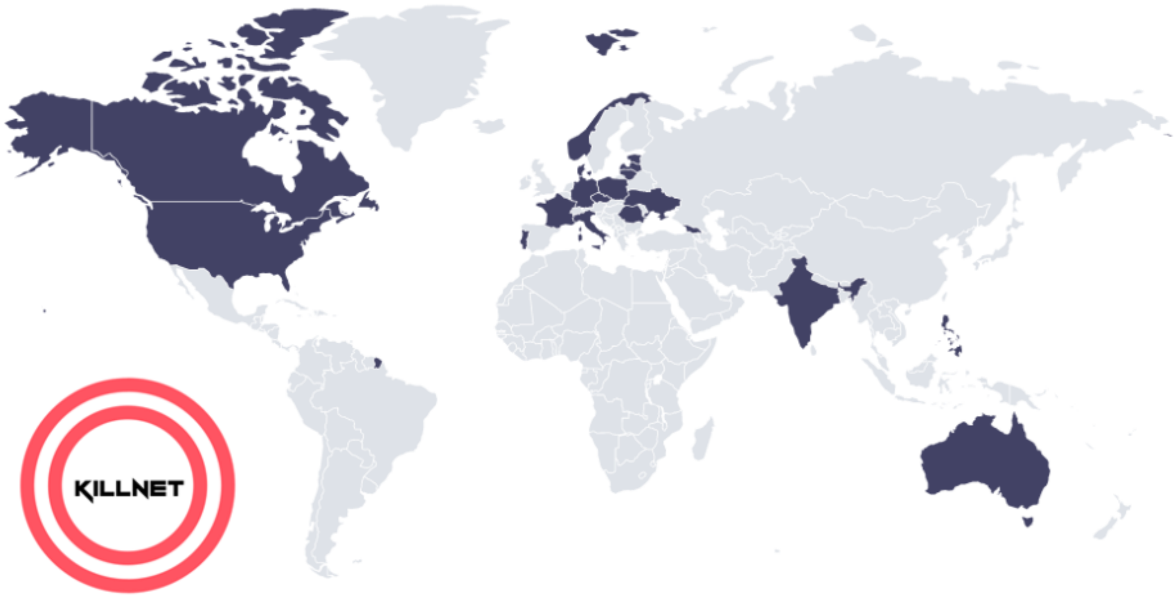
[redacted]

1.2K Nov 27 at 21:46

SOCRadar Threat Actors Module provides detailed information on threat actors, IoCs, and exploited CVEs.

Killnet's Targets and Operations

Killnet has attacked many **European and Western** countries, including Ukraine, since February 2022. The **US, the UK, Germany, Italy, Romania, Lithuania, Estonia, and Poland** are among these. Attacks on US airports, the **Eurovision contest** website, and more than a thousand websites in Lithuania were worth mentioning. There were also attacks on railways and government portals in the Czech Republic.



Countries affected by Killnet (Source: SOCRadar)

In April 2022, Killnet focused entirely on supporting Russian geopolitical interests worldwide. They claimed to have carried out more than **550 attacks** between late February and September. Only 45 of these attacks were directed against Ukraine, **less than 10%** of the total attacks.

You can find previous attacks of Killnet on SOCRadar's research article published on July 28, 2022.

Killnet's Recent Cyber Attacks

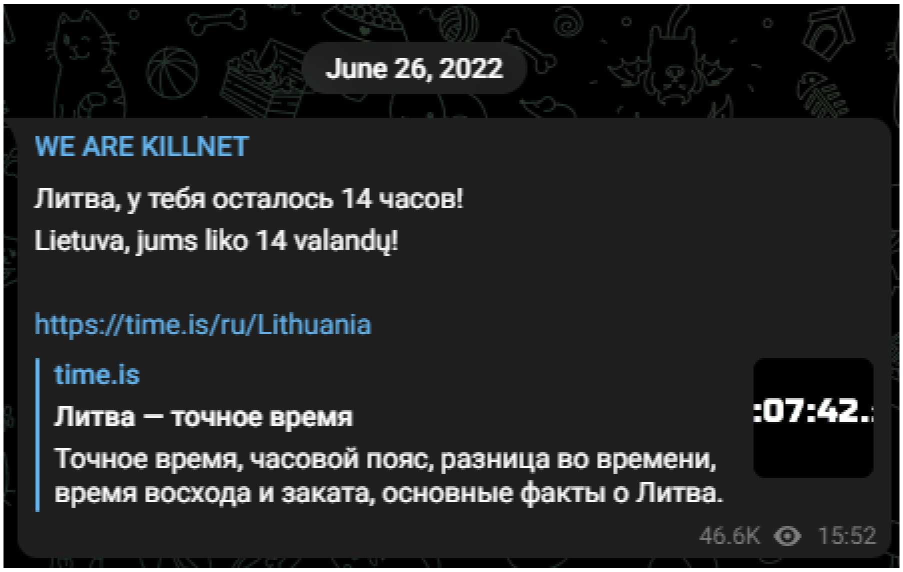
May 2022:

Killnet attacked Romanian government websites.

They attacked Italy and managed to block a few websites, while the attack on the **CSIRT** site was unsuccessful. Killnet hacked **Istituto Superiore di Sanità** and the **Automobile Club of Italy** websites in the same attack. The Italian Senate website was also hacked and closed for an hour. The attack was not as devastating as predicted.

June 2022:

The group targeted **Norwegian organizations** through various DDoS attacks. Also, the group took responsibility for the DDoS attack through the Lithuanian government and private institutions.



June 26, 2022

WE ARE KILLNET

Литва, у тебя осталось 14 часов!
Lietuva, jums liko 14 valandų!

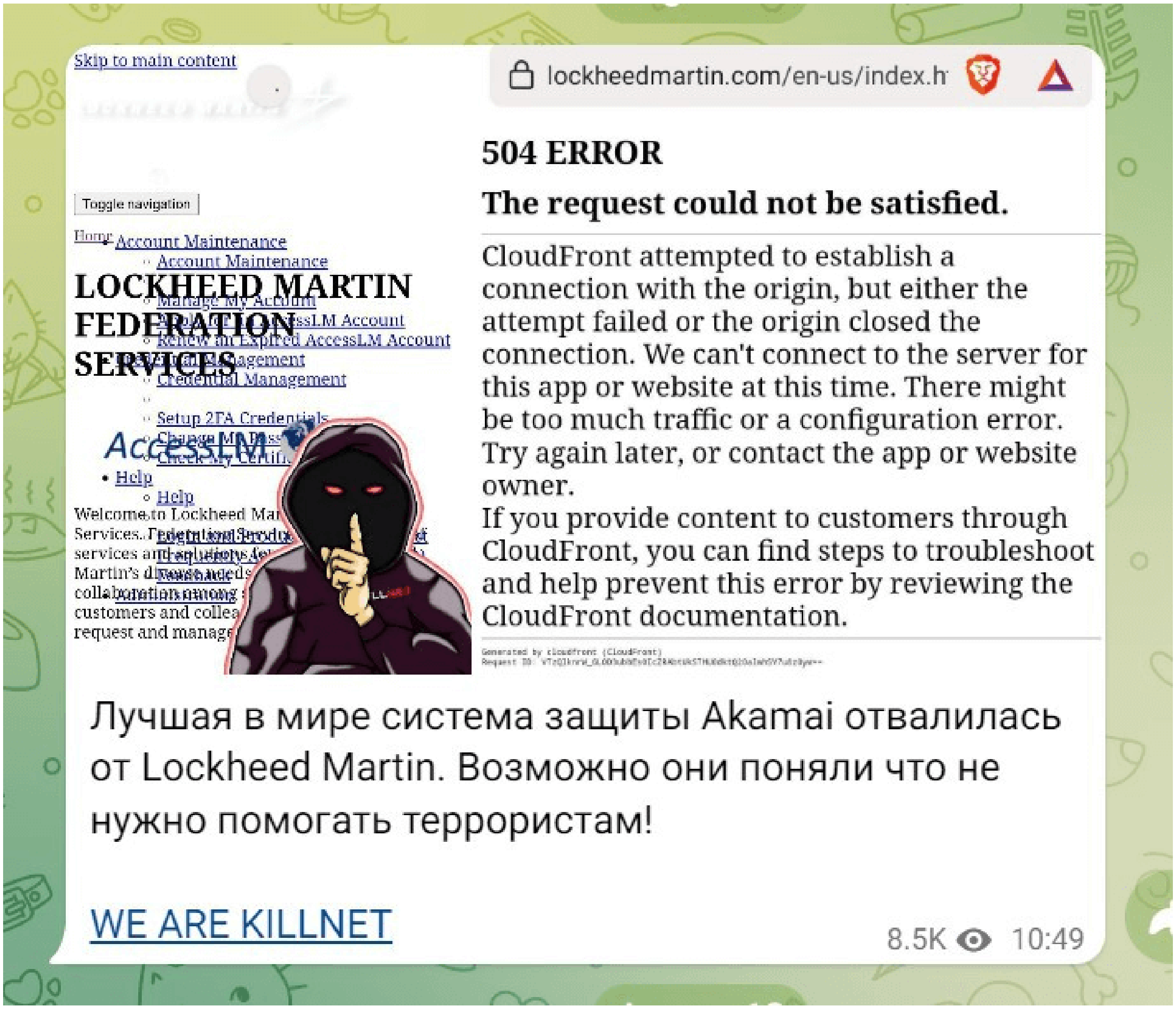
https://time.is/ru/Lithuania

time.is
Литва — точное время
Точное время, часовой пояс, разница во времени, время восхода и заката, основные факты о Литва.

46.6K 15:52

August 2022:

The group and its founder, called “**KillMilk**,” claimed responsibility for a cyber-attack on the American defense contractor **Lockheed Martin** as a retaliation for the HIMARS systems supplied by the US to Ukraine.



LOCKHEED MARTIN FEDERATION SERVICES

Welcome to Lockheed Mar
Services. Federation Servic
services and solutions fo
Martin's diverse needs
collaboration among
customers and collea
request and manage

504 ERROR

The request could not be satisfied.

CloudFront attempted to establish a connection with the origin, but either the attempt failed or the origin closed the connection. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner.
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.

Generated by cloudfront (CloudFront)

Лучшая в мире система защиты Akamai отвалилась от Lockheed Martin. Возможно они поняли что не нужно помогать террористам!

WE ARE KILLNET

8.5K 10:49

September 2022:

Killnet announced that it had attacked **23 websites of 4 ministries** and agencies in Japan, including e-Gov, a portal site for administrative information administered by the Digital Agency, and eLTAX, a local tax website administered by the **Ministry of Internal Affairs and Communications**.

October 2022:

Several US airport websites were attacked.

Killnet posted a list of several government websites they would target in the coming days beneath an image of a nuclear explosion behind the Statue of Liberty.

Alleged targets are listed below:

- Alabama
- Alaska
- Connecticut
- Colorado
- Delaware
- Florida
- Hawaii
- Idaho
- Indiana
- Kansas
- Kentucky
- Mississippi

November 2022:

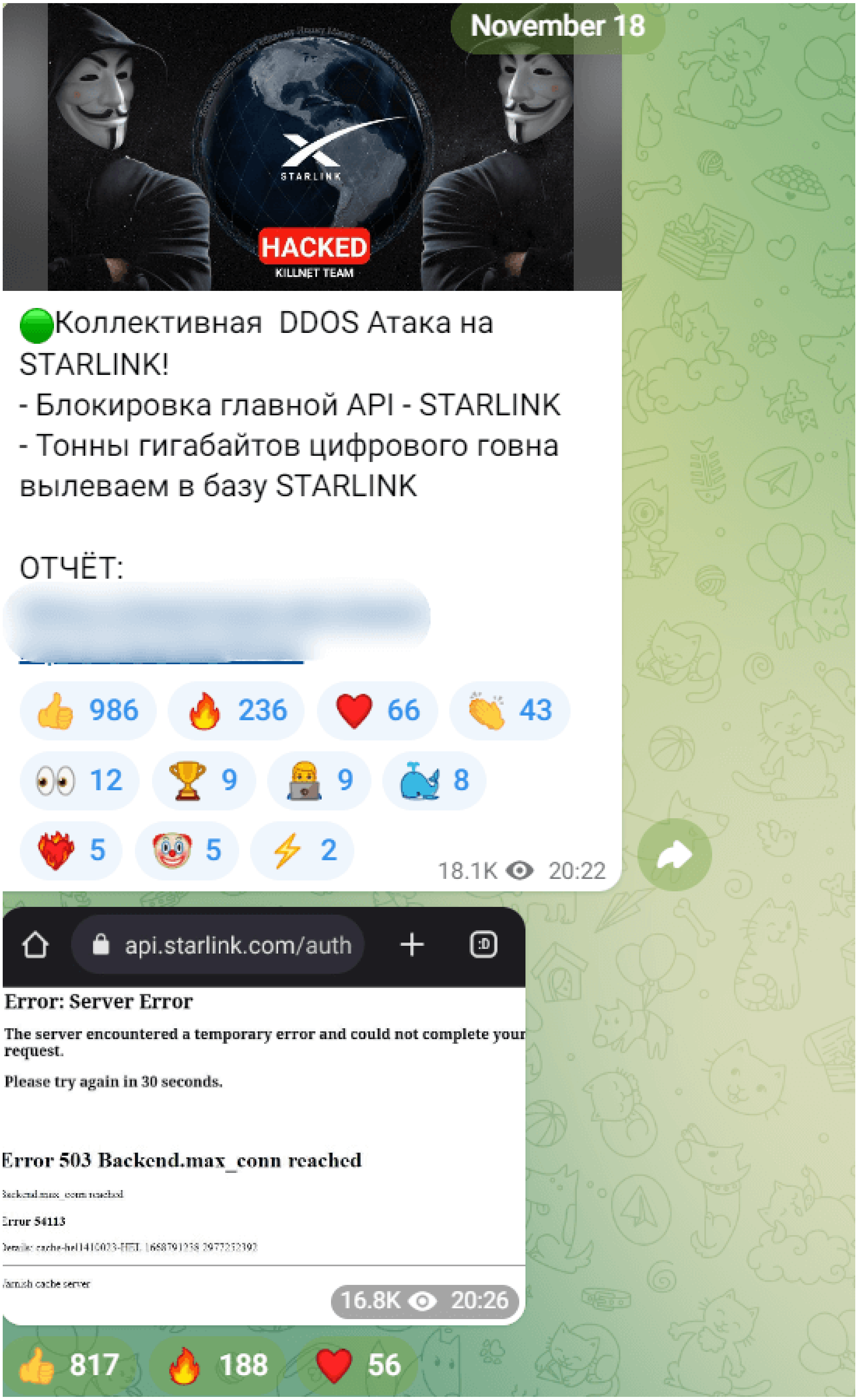
On the Killnet Telegram channel, the group shared a post that said, “We have gained strength and now we are able to reduce the traffic of drug addicts to sellers’ websites to zero! Not without your help, of course, comrades!”

Killnet threat actors hacked Russia’s largest dark web drug site. They published dealers’ and drug addicts’ data, storage locations, etc.

In a mail from a Latvian State Revenue Service employee, they announced they have VPN access to corporate government networks and downloaded **200 gigabytes** of documents.

Killnet hacker group declared that they attacked western governments' and companies' websites. They have posted a gateway to **a government portal** for authentication and access to various web resources in their Telegram group.

The **White House** announced that it has temporarily closed its official website and **Starlink API**. Experts stated it is a critical target because the Ukrainian army uses Starlink



November 18

🟢Коллективная DDOS Атака на STARLINK!
- Блокировка главной API - STARLINK
- Тонны гигабайтов цифрового говна вылеваем в базу STARLINK

ОТЧЁТ:
[redacted]

👍 986 🔥 236 ❤️ 66 👏 43
👀 12 🏆 9 👩‍💻 9 🐳 8
❤️‍🔥 5 🤡 5 ⚡ 2

18.1K 👁 20:22

api.starlink.com/auth

Error: Server Error

The server encountered a temporary error and could not complete your request.

Please try again in 30 seconds.

Error 503 Backend.max_conn reached

Backend.max_conn reached

Error 54113

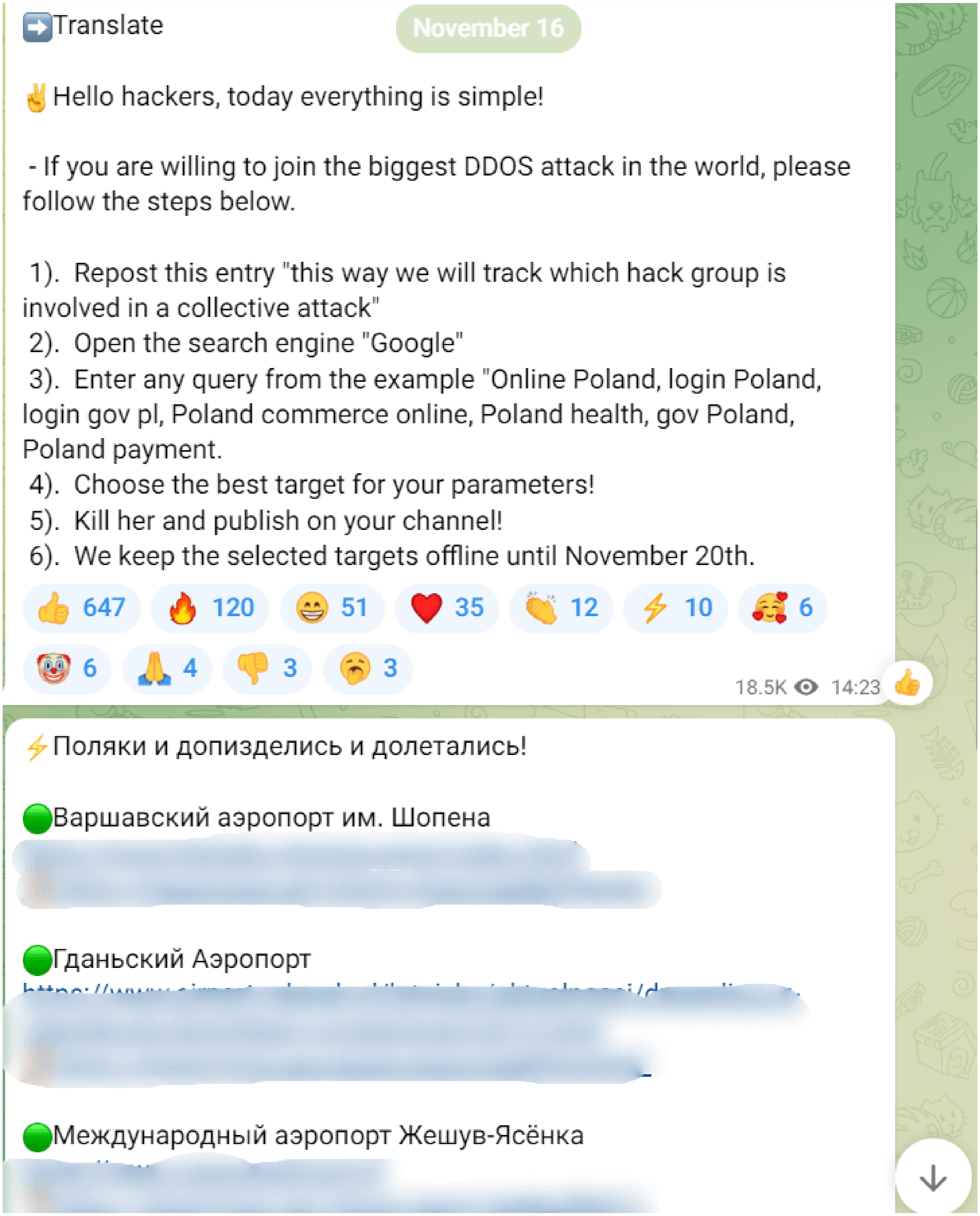
Details: cache-hel1410023-HEL 1668791238 2977252392

Varnish cache server

16.8K 👁 20:26

👍 817 🔥 188 ❤️ 56

Killnet posted an announcement on its Telegram channel, asking all hackers for help attacking and targeting Poland. They said several of the targets would be inoperable for four days. Following this announcement, Warsaw Airport, Gdansk Airport, and Rzeszow Airport became victims of cyberattacks.



✌️Hello hackers, today everything is simple!

- If you are willing to join the biggest DDOS attack in the world, please follow the steps below.

1). Repost this entry "this way we will track which hack group is involved in a collective attack"
2). Open the search engine "Google"
3). Enter any query from the example "Online Poland, login Poland, login gov pl, Poland commerce online, Poland health, gov Poland, Poland payment.
4). Choose the best target for your parameters!
5). Kill her and publish on your channel!
6). We keep the selected targets offline until November 20th.

⚡Поляки и допизделись и долетались!

🟢Варшавский аэропорт им. Шопена
[redacted]

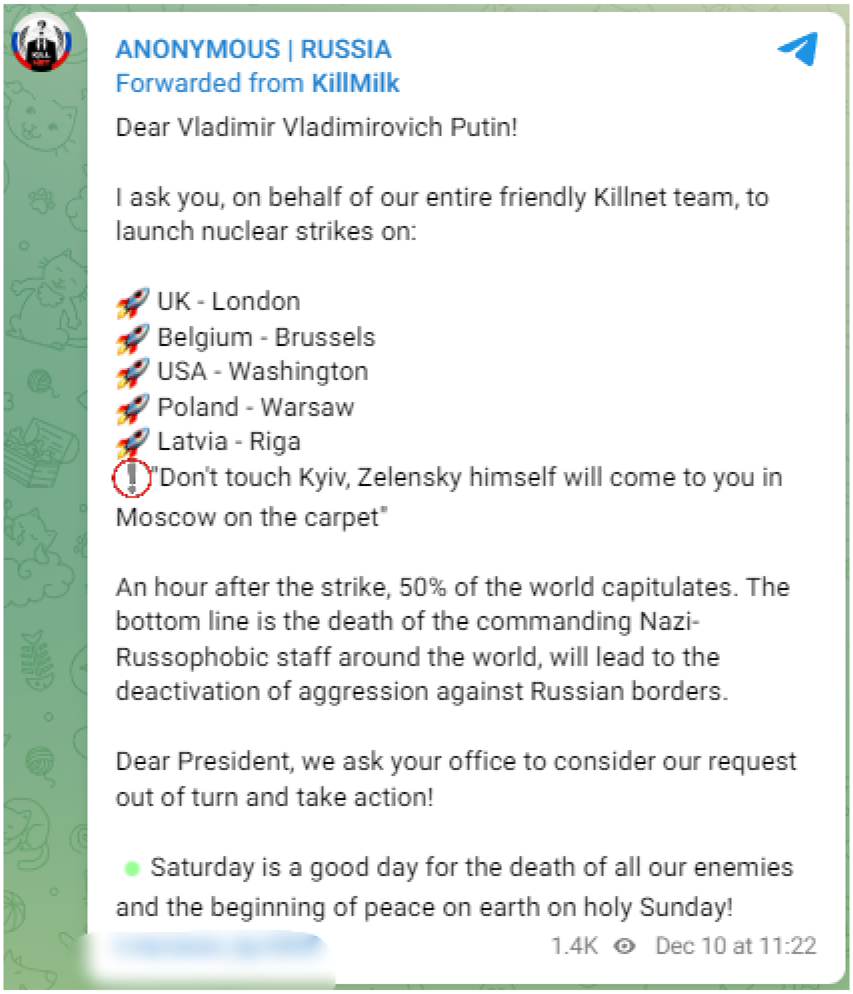
🟢Гданьский Аэропорт
[redacted]

🟢Международный аэропорт Жешув-Ясёнка
[redacted]

December 2022:

In a post, the Killnet group mentioned a new project called Infinity. They plan to launch the project sometime this winter-spring, which is getting a lot of attention at this stage.

They have also published a post asking President Putin for nuclear strikes on the capitals of Ukraine's allies on the Killnet telegram channel:



ANONYMOUS | RUSSIA
Forwarded from KillMilk

Dear Vladimir Vladimirovich Putin!

I ask you, on behalf of our entire friendly Killnet team, to launch nuclear strikes on:

🚀 UK - London
🚀 Belgium - Brussels
🚀 USA - Washington
🚀 Poland - Warsaw
🚀 Latvia - Riga
❕"Don't touch Kyiv, Zelensky himself will come to you in Moscow on the carpet"

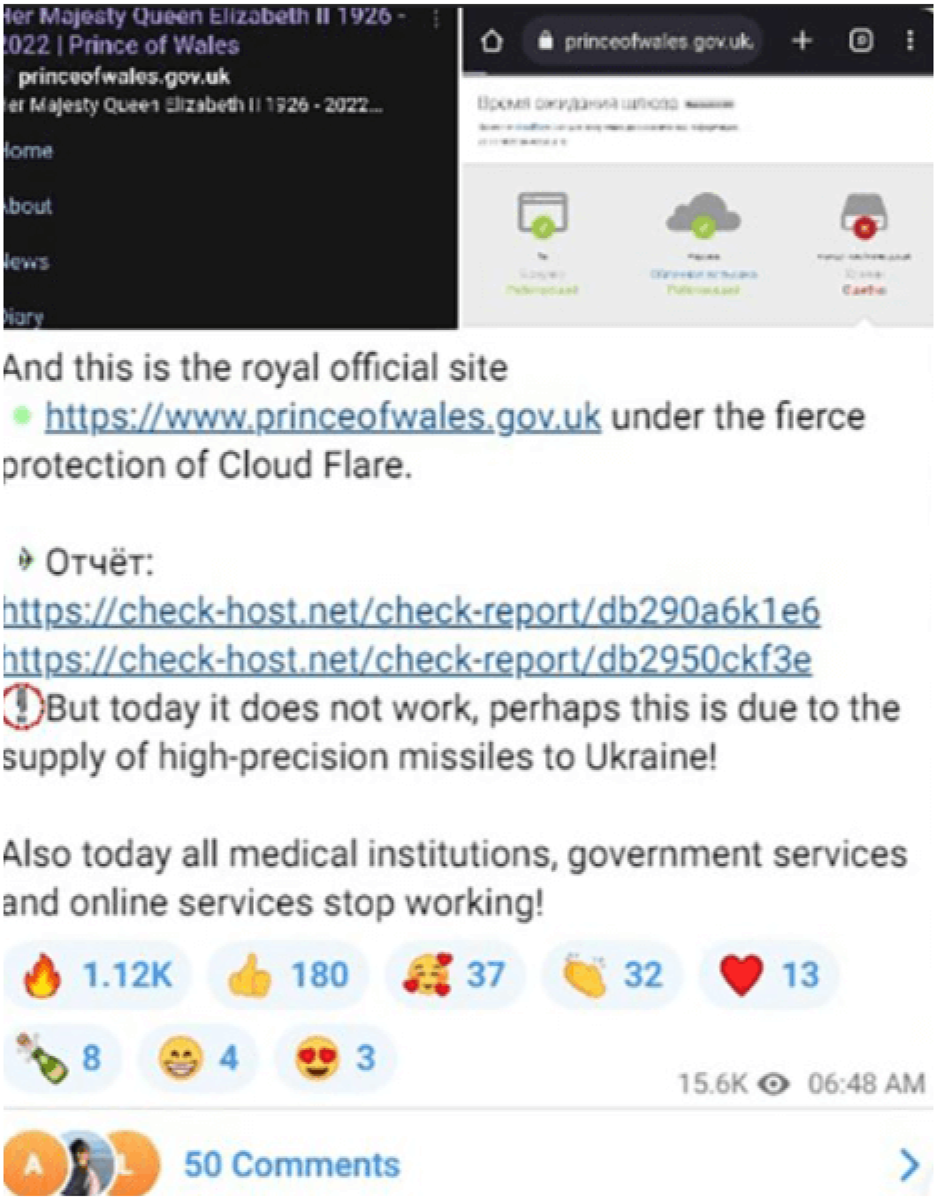
An hour after the strike, 50% of the world capitulates. The bottom line is the death of the commanding Nazi-Russophobic staff around the world, will lead to the deactivation of aggression against Russian borders.

Dear President, we ask your office to consider our request out of turn and take action!

🟢 Saturday is a good day for the death of all our enemies and the beginning of peace on earth on holy Sunday!

[redacted] 1.4K 👁 Dec 10 at 11:22

Another critical piece of intelligence about the Killnet group is that some members said they attacked the Bankers Automated Clearing Service (BACS), the London Stock Exchange, and the Prince of Wales official website. Killnet stated that the "royal official site" was not working. "Perhaps this is due to the supply of high-precision missiles to Ukraine," the group said.


ler Majesty Queen Elizabeth II 1926 -
022 | Prince of Wales
princeofwales.gov.uk
ler Majesty Queen Elizabeth II 1926 - 2022...
lome
bout
lews
liary
princeofwales.gov.uk

And this is the royal official site
● https://www.princeofwales.gov.uk under the fierce protection of Cloud Flare.

Отчёт:
https://check-host.net/check-report/db290a6k1e6
https://check-host.net/check-report/db2950ckf3e
❗But today it does not work, perhaps this is due to the supply of high-precision missiles to Ukraine!

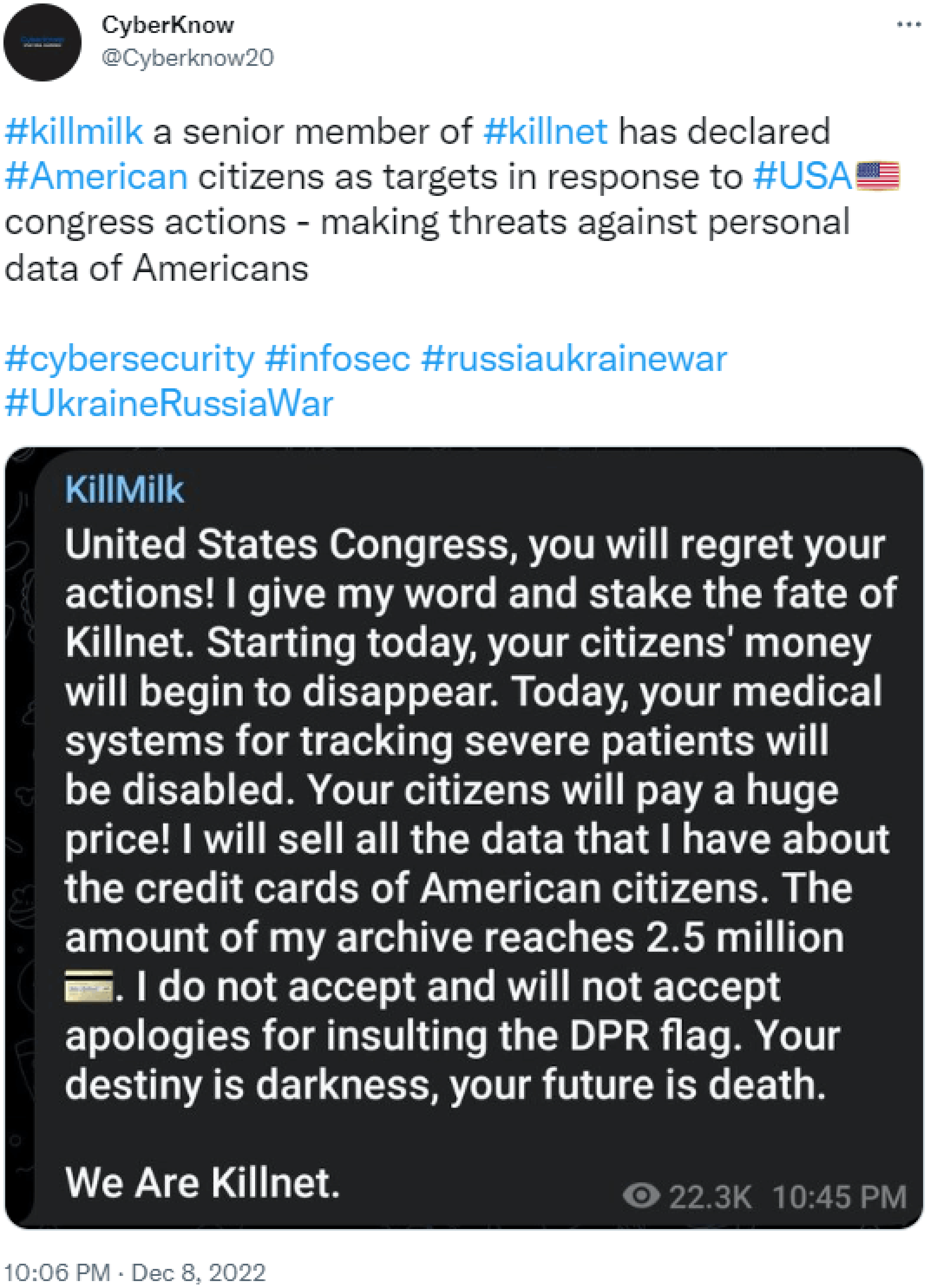
Also today all medical institutions, government services and online services stop working!

🔥 1.12K 👍 180 🥰 37 👏 32 ❤️ 13
🍾 8 😁 4 😍 3

15.6K 👁 06:48 AM

50 Comments

Killmilk, a senior member of the Killnet group, has threatened the **US Congress** with the sale of the health and personal data of the American people because of the Ukraine policy of the US Congress.



CyberKnow
@Cyberknow20

#killmilk a senior member of #killnet has declared #American citizens as targets in response to #USA🇺🇸 congress actions - making threats against personal data of Americans

#cybersecurity #infosec #russiaukrainewar #UkraineRussiaWar

KillMilk

United States Congress, you will regret your actions! I give my word and stake the fate of Killnet. Starting today, your citizens' money will begin to disappear. Today, your medical systems for tracking severe patients will be disabled. Your citizens will pay a huge price! I will sell all the data that I have about the credit cards of American citizens. The amount of my archive reaches 2.5 million 💳. I do not accept and will not accept apologies for insulting the DPR flag. Your destiny is darkness, your future is death.

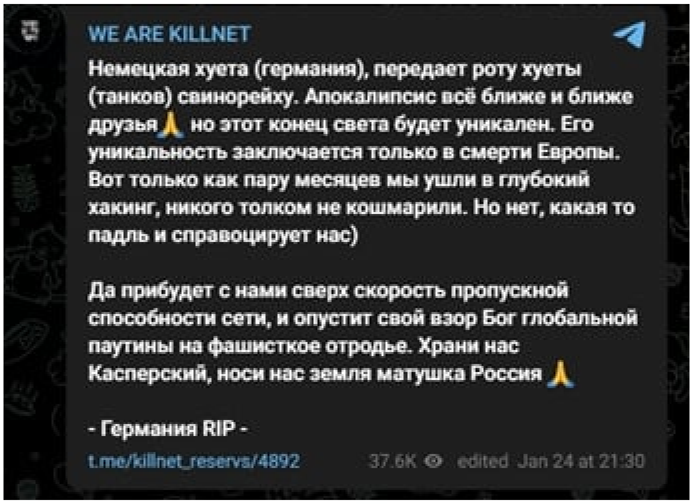
We Are Killnet.

22.3K 10:45 PM

10:06 PM · Dec 8, 2022

January 2023:

In late January 2023, KillNet shared that it was targeting Germany via the **Passion Botnet** with the hashtag #ГерманияRIP.



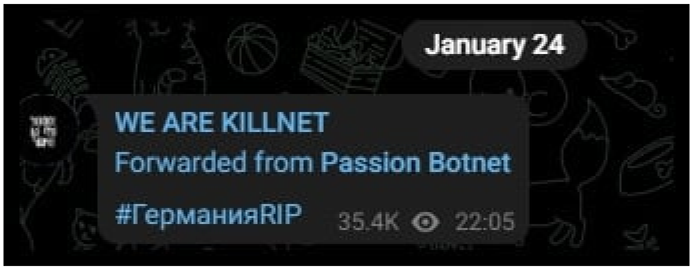
WE ARE KILLNET

Немецкая хуета (германия), передает роту хуеты (танков) свинорейху. Апокалипсис всё ближе и ближе друзья🙏 но этот конец света будет уникален. Его уникальность заключается только в смерти Европы. Вот только как пару месяцев мы ушли в глубокий хакинг, никого толком не кошмарили. Но нет, какая то падль и справоцирует нас)

Да прибудет с нами сверх скорость пропускной способности сети, и опустит свой взор Бог глобальной паутины на фашисткое отродье. Храни нас Касперский, носи нас земля матушка Россия🙏

- Германия RIP -

t.me/killnet_reservs/4892 37.6K edited Jan 24 at 21:30

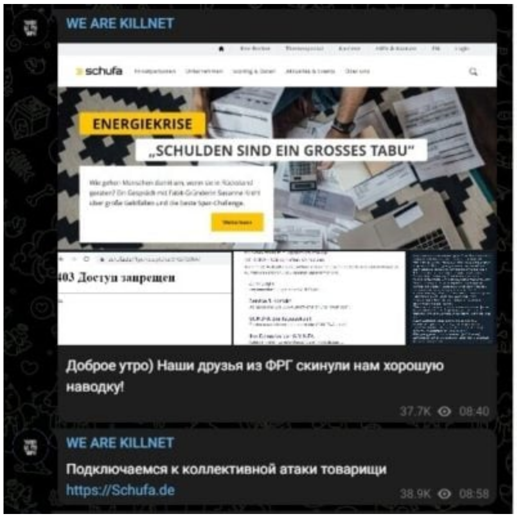


January 24

WE ARE KILLNET
Forwarded from Passion Botnet

#ГерманияRIP 35.4K 22:05

A day after the announcement, the group posted screenshots showing that they had denied access to several German websites, including the Cabinet of Germany (**Bundesregierung**) and the Federal Ministry of the Interior (**Bundesministerium des Innern und für Heimat**).



WE ARE KILLNET

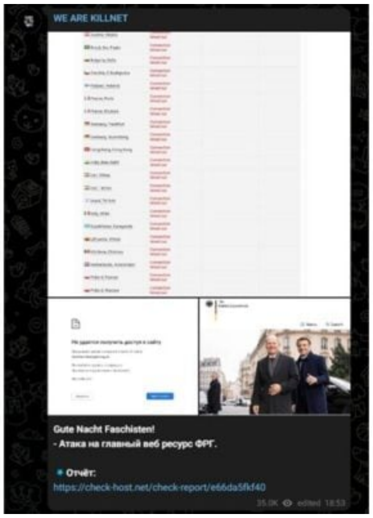
Доброе утро) Наши друзья из ФРГ скинули нам хорошую наводку!

37.7K 08:40

WE ARE KILLNET

Подключаемся к коллективной атаки товарищи
https://Schufa.de

38.9K 08:58

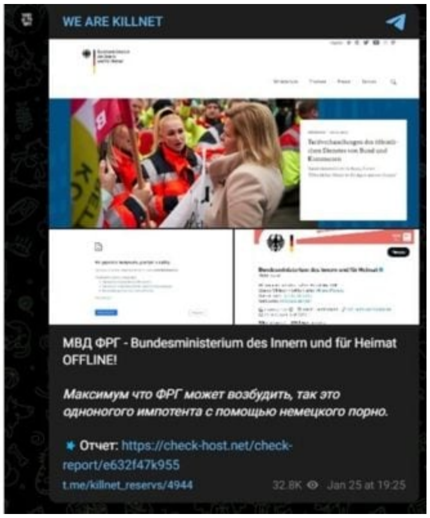


WE ARE KILLNET

Gute Nacht Faschisten!
- Атака на главный веб ресурс ФРГ.

Отчёт:
https://check-host.net/check-report/e66da5fkf40

35.0K edited 18:53



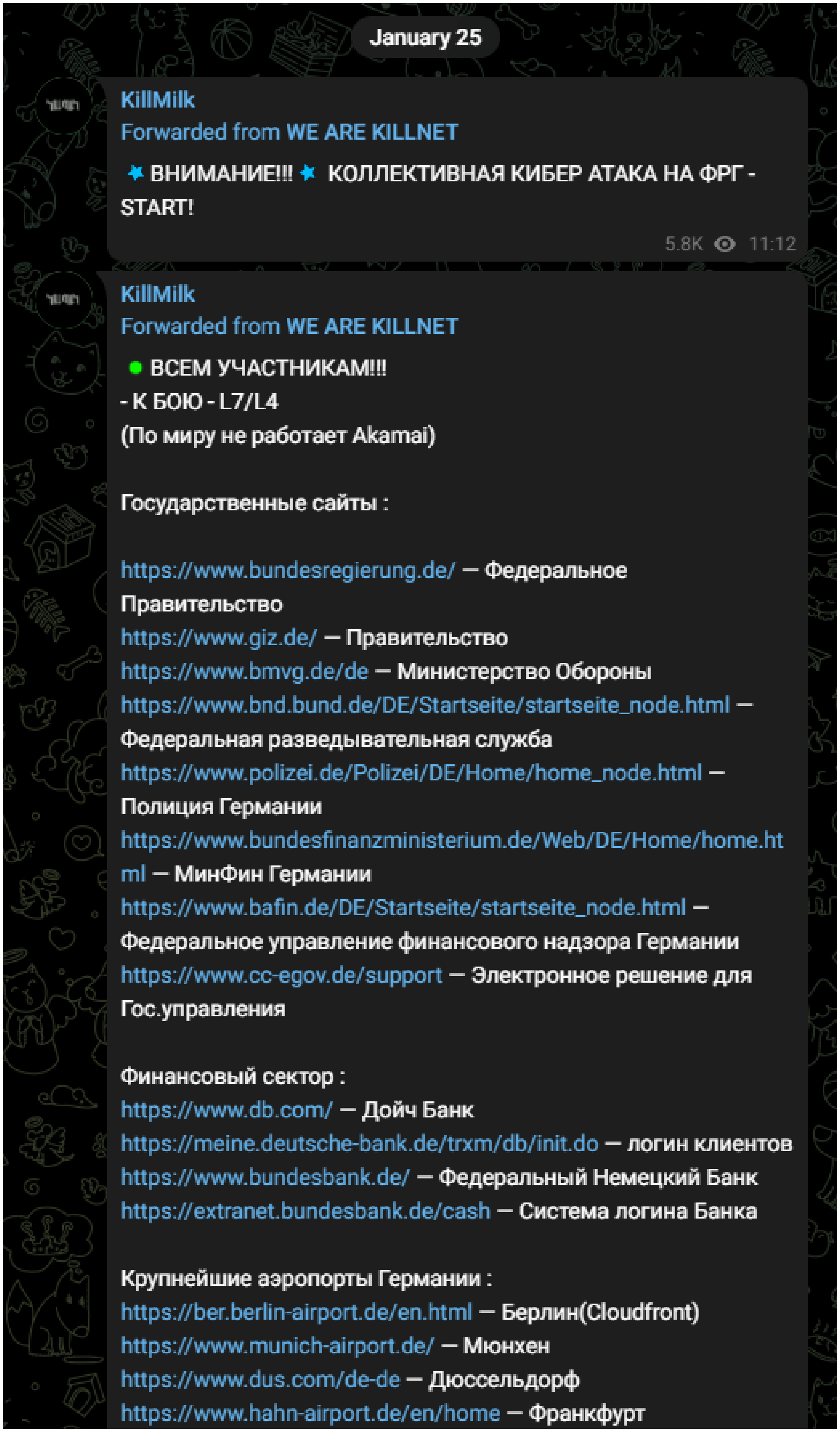
WE ARE KILLNET

МВД ФРГ - Bundesministerium des Innern und für Heimat OFFLINE!

Максимум что ФРГ может возбудить, так это одноногого импотента с помощью немецкого порно.

Отчет: https://check-host.net/check-report/e632f47k955
t.me/killnet_reservs/4944 32.8K Jan 25 at 19:25

Killnet shared a list of other German websites they targeted on the same day, categorized by industry:



January 25

KillMilk
Forwarded from WE ARE KILLNET

✴ ВНИМАНИЕ!!! ✴ КОЛЛЕКТИВНАЯ КИБЕР АТАКА НА ФРГ - START!

5.8K 👁 11:12

KillMilk
Forwarded from WE ARE KILLNET

🟢 ВСЕМ УЧАСТНИКАМ!!!
- К БОЮ - L7/L4
(По миру не работает Akamai)

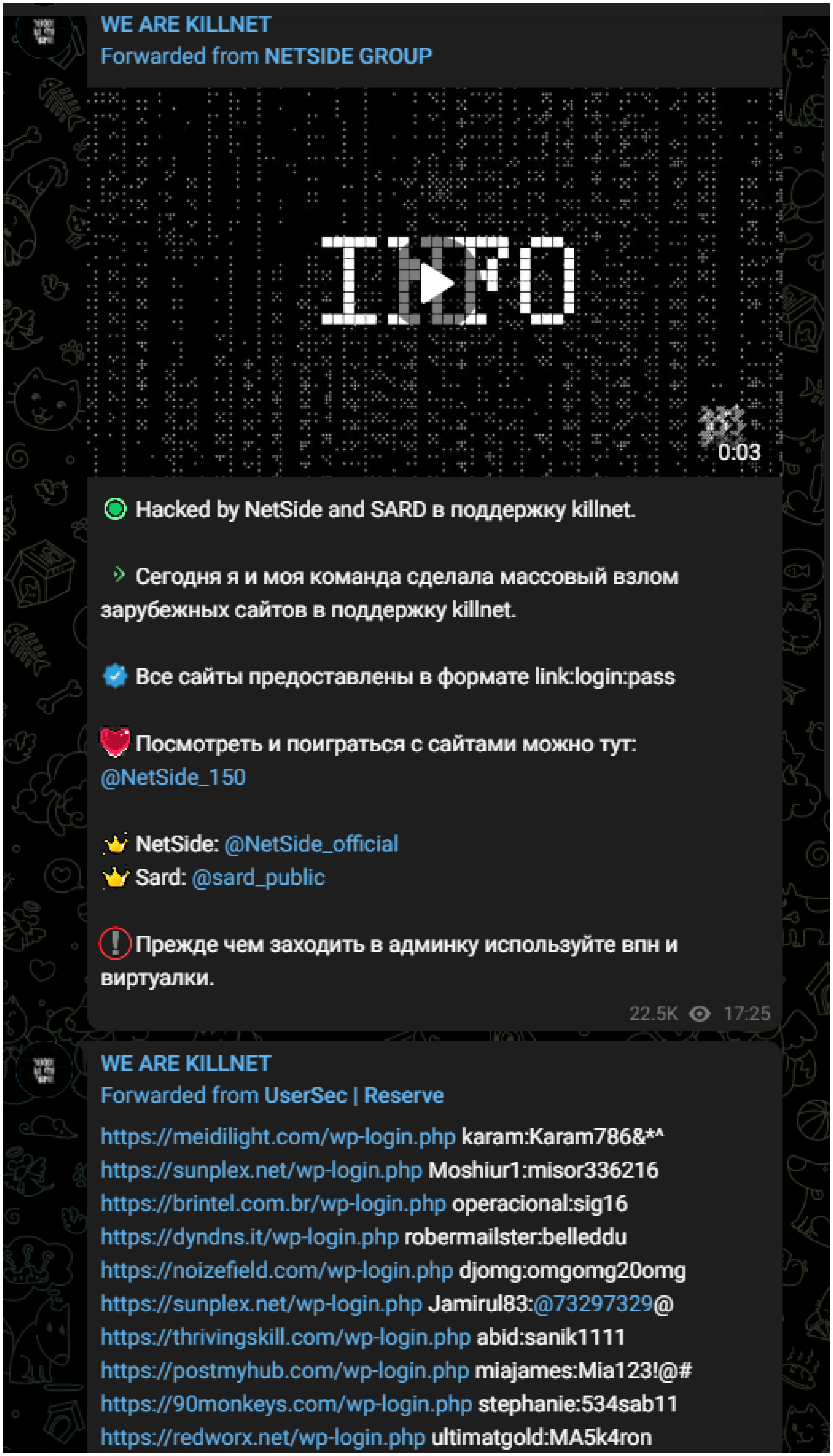
Государственные сайты :

https://www.bundesregierung.de/ — Федеральное Правительство
https://www.giz.de/ — Правительство
https://www.bmvg.de/de — Министерство Обороны
https://www.bnd.bund.de/DE/Startseite/startseite_node.html — Федеральная разведывательная служба
https://www.polizei.de/Polizei/DE/Home/home_node.html — Полиция Германии
https://www.bundesfinanzministerium.de/Web/DE/Home/home.html — МинФин Германии
https://www.bafin.de/DE/Startseite/startseite_node.html — Федеральное управление финансового надзора Германии
https://www.cc-egov.de/support — Электронное решение для Гос.управления

Финансовый сектор :
https://www.db.com/ — Дойч Банк
https://meine.deutsche-bank.de/trxm/db/init.do — логин клиентов
https://www.bundesbank.de/ — Федеральный Немецкий Банк
https://extranet.bundesbank.de/cash — Система логина Банка

Крупнейшие аэропорты Германии :
https://ber.berlin-airport.de/en.html — Берлин(Cloudfront)
https://www.munich-airport.de/ — Мюнхен
https://www.dus.com/de-de — Дюссельдорф
https://www.hahn-airport.de/en/home — Франкфурт

The **NetSide and SARD Telegram groups** also shared that they had hacked the admin panels of hundreds of websites to support Killnet and posted the credentials on Killnet’s page:



WE ARE KILLNET
Forwarded from NETSIDE GROUP

🟢 Hacked by NetSide and SARD в поддержку killnet.

› Сегодня я и моя команда сделала массовый взлом зарубежных сайтов в поддержку killnet.

✅ Все сайты предоставлены в формате link:login:pass

❤️ Посмотреть и поиграться с сайтами можно тут: @NetSide_150

👑 NetSide: @NetSide_official
👑 Sard: @sard_public

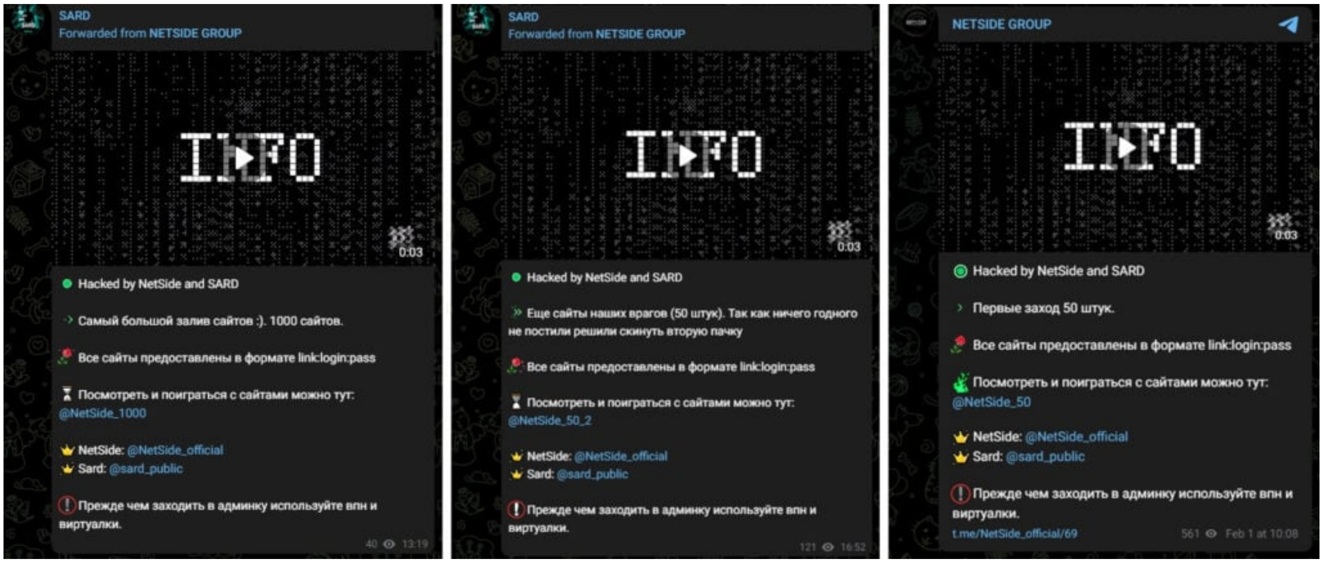
❗ Прежде чем заходить в админку используйте впн и виртуалки.

22.5K 17:25

WE ARE KILLNET
Forwarded from UserSec | Reserve

https://meidilight.com/wp-login.php karam:Karam786&*^
https://sunplex.net/wp-login.php Moshiur1:misor336216
https://brintel.com.br/wp-login.php operacional:sig16
https://dyndns.it/wp-login.php robermailster:belleddu
https://noizefield.com/wp-login.php djomg:omgomg20omg
https://sunplex.net/wp-login.php Jamirul83:@73297329@
https://thrivingskill.com/wp-login.php abid:sanik1111
https://postmyhub.com/wp-login.php miajames:Mia123!@#
https://90monkeys.com/wp-login.php stephanie:534sab11
https://redworx.net/wp-login.php ultimatgold:MA5k4ron

It is noteworthy that NetSide and SARD make such posts at regular intervals.



SARD
Forwarded from NETSIDE GROUP

● Hacked by NetSide and SARD

› Самый большой залив сайтов :). 1000 сайтов.

🌹 Все сайты предоставлены в формате link:login:pass

⏳ Посмотреть и поиграться с сайтами можно тут:
@NetSide_1000

👑 NetSide: @NetSide_official
👑 Sard: @sard_public

❗ Прежде чем заходить в админку используйте впн и виртуалки.

40 👁 13:19

SARD
Forwarded from NETSIDE GROUP

● Hacked by NetSide and SARD

» Еще сайты наших врагов (50 штук). Так как ничего годного не постили решили скинуть вторую пачку

🌹 Все сайты предоставлены в формате link:login:pass

⏳ Посмотреть и поиграться с сайтами можно тут:
@NetSide_50_2

👑 NetSide: @NetSide_official
👑 Sard: @sard_public

❗ Прежде чем заходить в админку используйте впн и виртуалки.

121 👁 16:52

NETSIDE GROUP

● Hacked by NetSide and SARD

› Первые заход 50 штук.

🌹 Все сайты предоставлены в формате link:login:pass

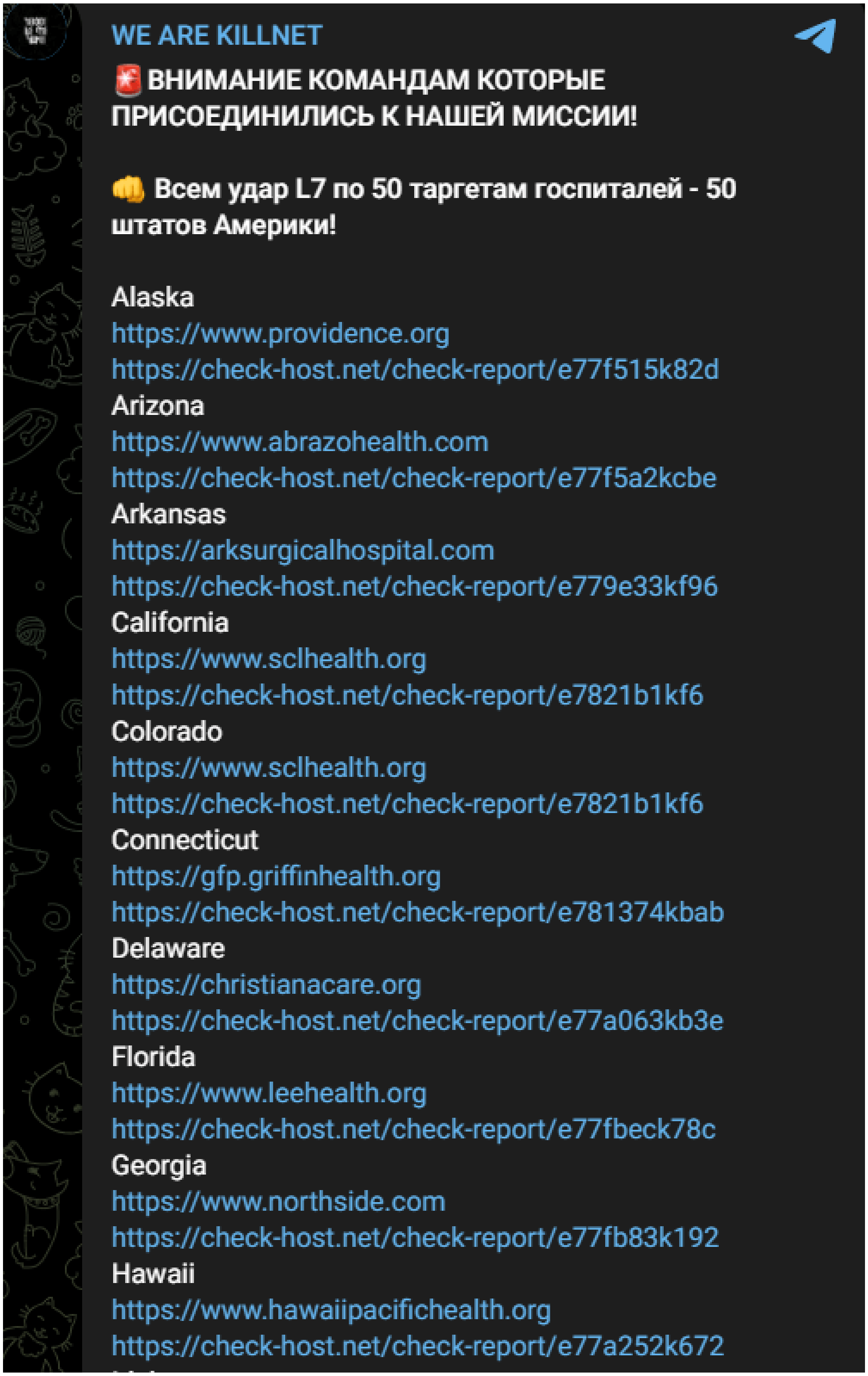
Посмотреть и поиграться с сайтами можно тут:
@NetSide_50

👑 NetSide: @NetSide_official
👑 Sard: @sard_public

❗ Прежде чем заходить в админку используйте впн и виртуалки.
t.me/NetSide_official/69

561 👁 Feb 1 at 10:08

At the end of the month, Killnet shared that they carried out a massive **Layer 7 DDoS attack** on several healthcare organizations all over the US. In addition, according to the Daily Mail, hospitals in the Netherlands reportedly experienced a DDoS attack from Russian hacking groups.



WE ARE KILLNET

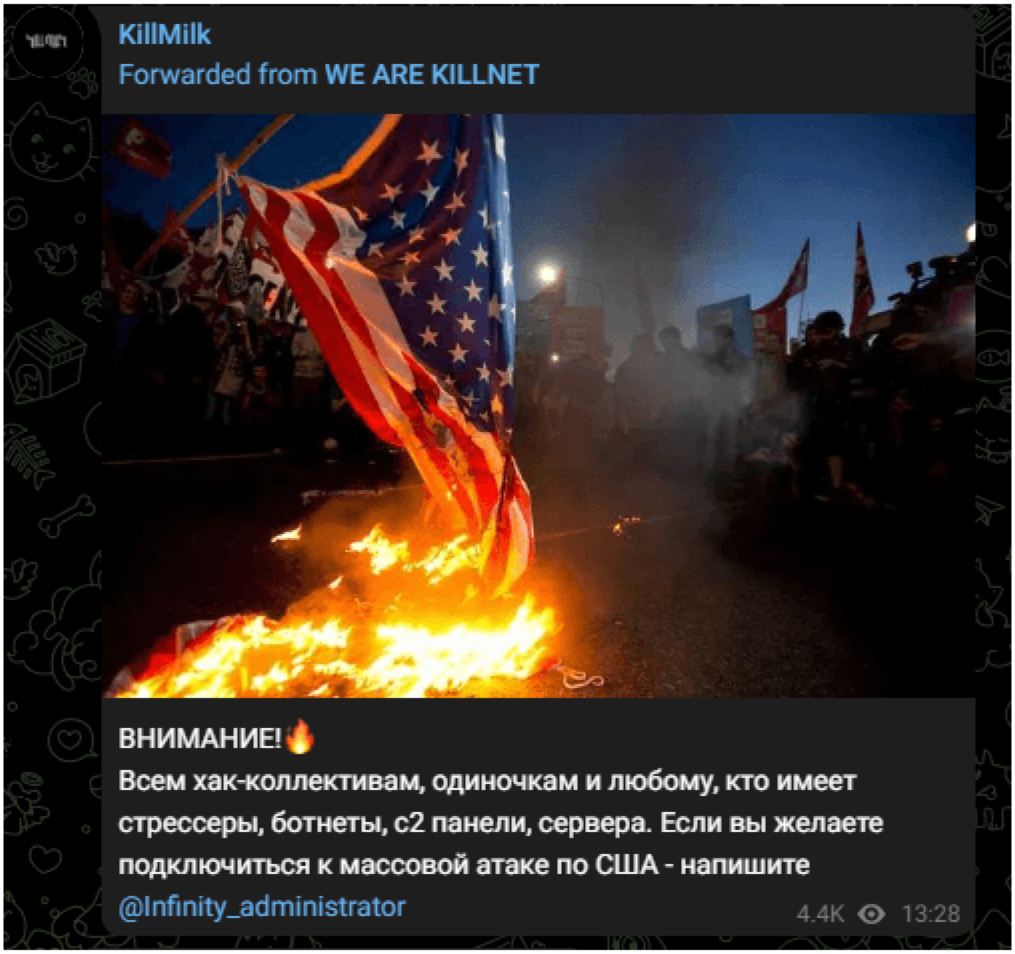
🚨 ВНИМАНИЕ КОМАНДАМ КОТОРЫЕ ПРИСОЕДИНИЛИСЬ К НАШЕЙ МИССИИ!

👊 Всем удар L7 по 50 таргетам госпиталей - 50 штатов Америки!

Alaska
https://www.providence.org
https://check-host.net/check-report/e77f515k82d
Arizona
https://www.abrazohealth.com
https://check-host.net/check-report/e77f5a2kcbe
Arkansas
https://arksurgicalhospital.com
https://check-host.net/check-report/e779e33kf96
California
https://www.sclhealth.org
https://check-host.net/check-report/e7821b1kf6
Colorado
https://www.sclhealth.org
https://check-host.net/check-report/e7821b1kf6
Connecticut
https://gfp.griffinhealth.org
https://check-host.net/check-report/e781374kbab
Delaware
https://christianacare.org
https://check-host.net/check-report/e77a063kb3e
Florida
https://www.leehealth.org
https://check-host.net/check-report/e77fbeck78c
Georgia
https://www.northside.com
https://check-host.net/check-report/e77fb83k192
Hawaii
https://www.hawaiipacifichealth.org
https://check-host.net/check-report/e77a252k672

February 2023:

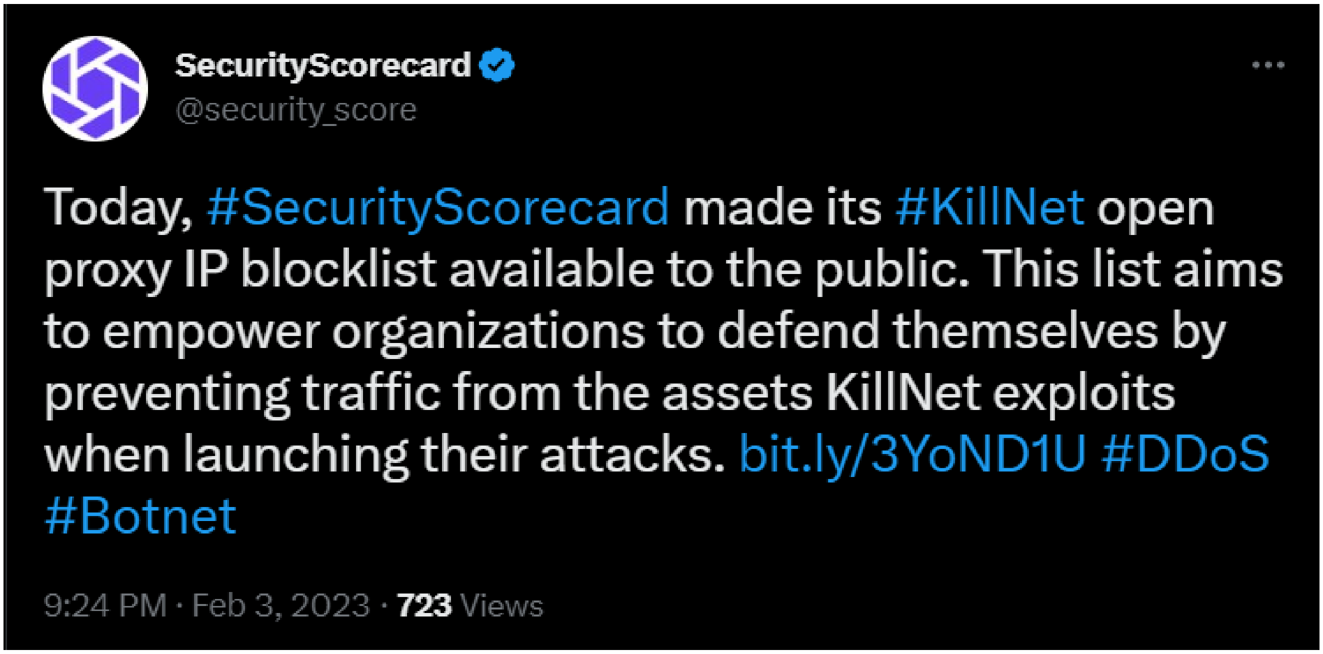
February started with a stunning announcement and a call to action; Killnet posted an announcement message urging anyone interested in attacking the United States to contact the administrator of the **Infinity hacker group**:



KillMilk
Forwarded from WE ARE KILLNET

ВНИМАНИЕ!🔥
Всем хак-коллективам, одиночкам и любому, кто имеет стрессеры, ботнеты, c2 панели, сервера. Если вы желаете подключиться к массовой атаке по США - напишите @Infinity_administrator

SecurityScorecard has shared a list of public IP addresses known to belong to Killnet so that cybersecurity personnel can block them:

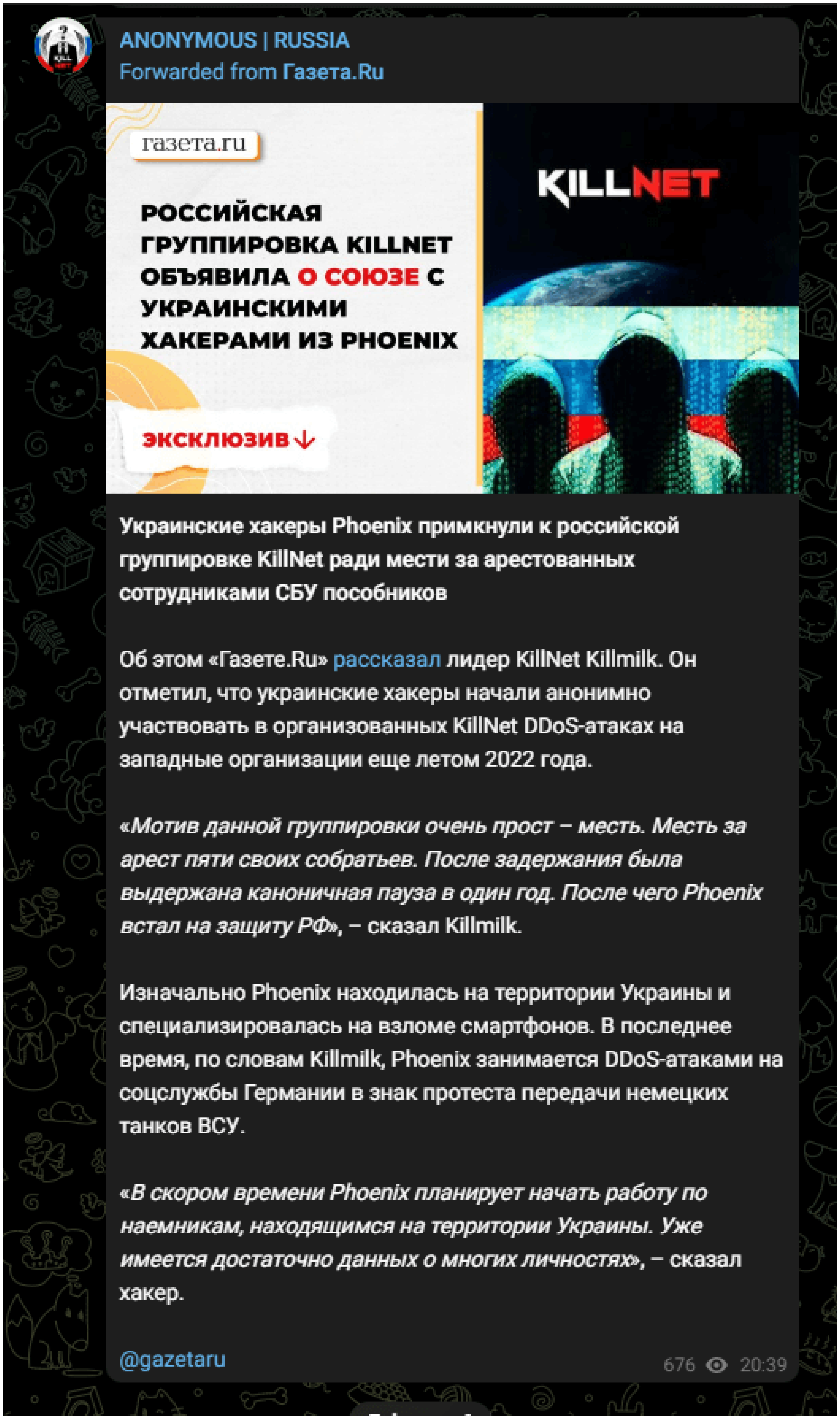


SecurityScorecard
@security_score

Today, #SecurityScorecard made its #KillNet open proxy IP blocklist available to the public. This list aims to empower organizations to defend themselves by preventing traffic from the assets KillNet exploits when launching their attacks. bit.ly/3YoND1U #DDoS #Botnet

9:24 PM · Feb 3, 2023 · 723 Views

Anonymous posted a news article from gazeta.ru on its Telegram channel about an interview with KillMilk, the leader of KillNet. According to KillMilk's interview, the Ukrainian hacking group Phoenix teamed up with the Russian group KillNet to take revenge for the arrest of their accomplices by the **SBU (Security Service of Ukraine)**:



ANONYMOUS | RUSSIA

Forwarded from Газета.Ru

газета.ru

РОССИЙСКАЯ ГРУППИРОВКА KILLNET ОБЪЯВИЛА О СОЮЗЕ С УКРАИНСКИМИ ХАКЕРАМИ ИЗ PHOENIX

ЭКСКЛЮЗИВ↓

KILLNET

Украинские хакеры Phoenix примкнули к российской группировке KillNet ради мести за арестованных сотрудниками СБУ пособников

Об этом «Газете.Ru» рассказал лидер KillNet Killmilk. Он отметил, что украинские хакеры начали анонимно участвовать в организованных KillNet DDoS-атаках на западные организации еще летом 2022 года.

«*Мотив данной группировки очень прост – месть. Месть за арест пяти своих собратьев. После задержания была выдержана каноничная пауза в один год. После чего Phoenix встал на защиту РФ*», – сказал Killmilk.

Изначально Phoenix находилась на территории Украины и специализировалась на взломе смартфонов. В последнее время, по словам Killmilk, Phoenix занимается DDoS-атаками на соцслужбы Германии в знак протеста передачи немецких танков ВСУ.

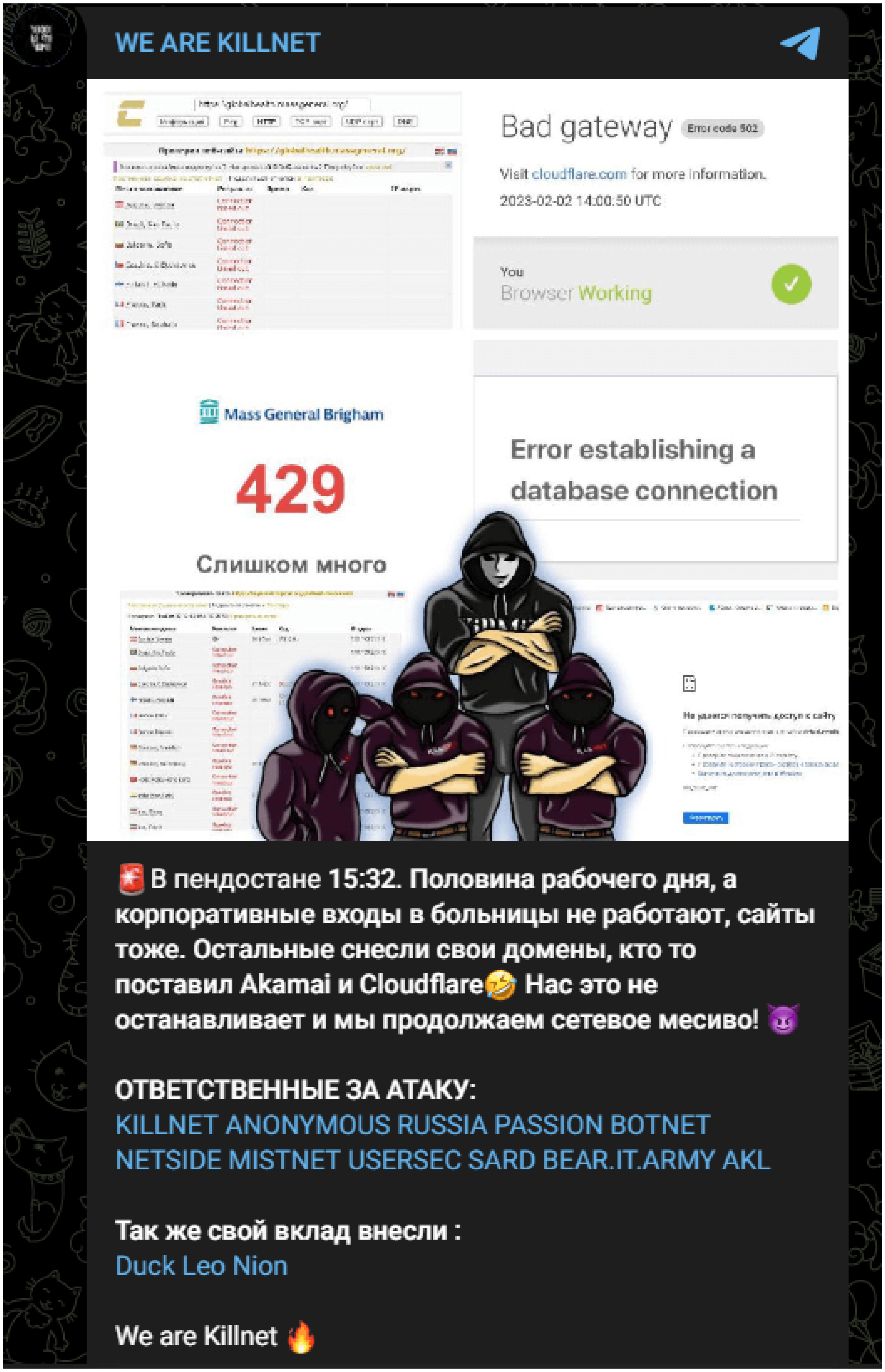
«*В скором времени Phoenix планирует начать работу по наемникам, находящимся на территории Украины. Уже имеется достаточно данных о многих личностях*», – сказал хакер.

@gazetaru

676 👁 20:39

Killnet in 2023

Since the end of January, Killnet has been actively targeting healthcare organizations. In their telegram post, they shared that the corporate entrances and websites of various hospitals were down and that this attack was a joint operation.



WE ARE KILLNET

Bad gateway Error code 502

Visit cloudflare.com for more information.

2023-02-02 14:00:50 UTC

You
Browser Working ✓

Mass General Brigham

429

Слишком много

Error establishing a database connection

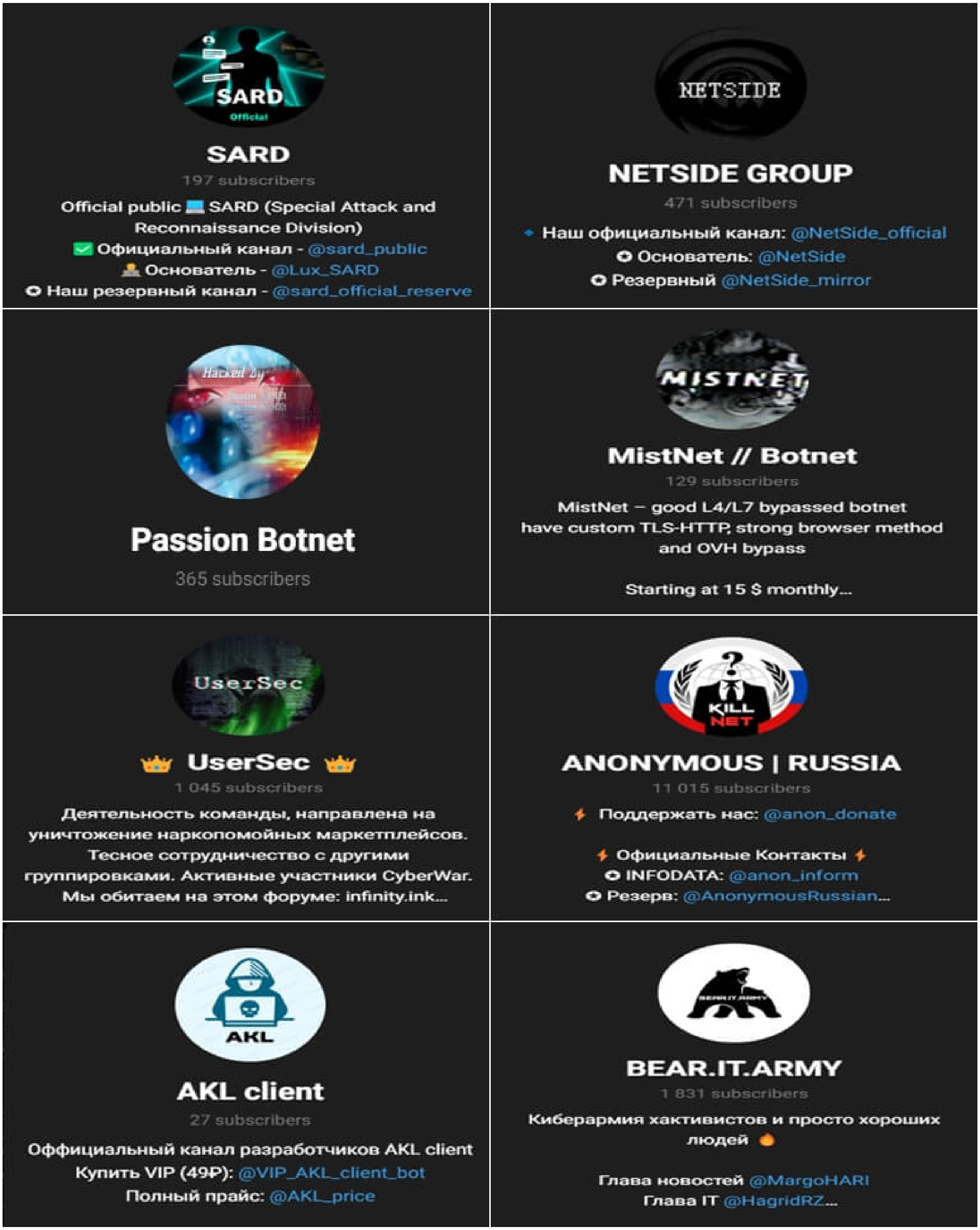
🚨 В пендостане 15:32. Половина рабочего дня, а корпоративные входы в больницы не работают, сайты тоже. Остальные снесли свои домены, кто то поставил Akamai и Cloudflare🤣 Нас это не останавливает и мы продолжаем сетевое месиво! 😈

ОТВЕТСТВЕННЫЕ ЗА АТАКУ:
KILLNET ANONYMOUS RUSSIA PASSION BOTNET NETSIDE MISTNET USERSEC SARD BEAR.IT.ARMY AKL

Так же свой вклад внесли :
Duck Leo Nion

We are Killnet 🔥

Some of those mentioned in KillNet’s Telegram post are hacker groups, and some are known as DDoS-as-a-Service providers.



SARD

197 subscribers

Official public SARD (Special Attack and Reconnaissance Division)
Официальный канал - @sard_public
Основатель - @Lux_SARD
Наш резервный канал - @sard_official_reserve

NETSIDE GROUP

471 subscribers

Наш официальный канал: @NetSide_official
Основатель: @NetSide
Резервный @NetSide_mirror

Passion Botnet

365 subscribers

MistNet // Botnet

129 subscribers

MistNet – good L4/L7 bypassed botnet
have custom TLS-HTTP, strong browser method and OVH bypass

Starting at 15 $ monthly...

👑 UserSec 👑

1 045 subscribers

Деятельность команды, направлена на уничтожение наркопомойных маркетплейсов. Тесное сотрудничество с другими группировками. Активные участники CyberWar. Мы обитаем на этом форуме: infinity.ink...

ANONYMOUS | RUSSIA

11 015 subscribers

Поддержать нас: @anon_donate

Официальные Контакты
INFODATA: @anon_inform
Резерв: @AnonymousRussian...

AKL client

27 subscribers

Оффициальный канал разработчиков AKL client
Купить VIP (49₽): @VIP_AKL_client_bot
Полный прайс: @AKL_price

BEAR.IT.ARMY

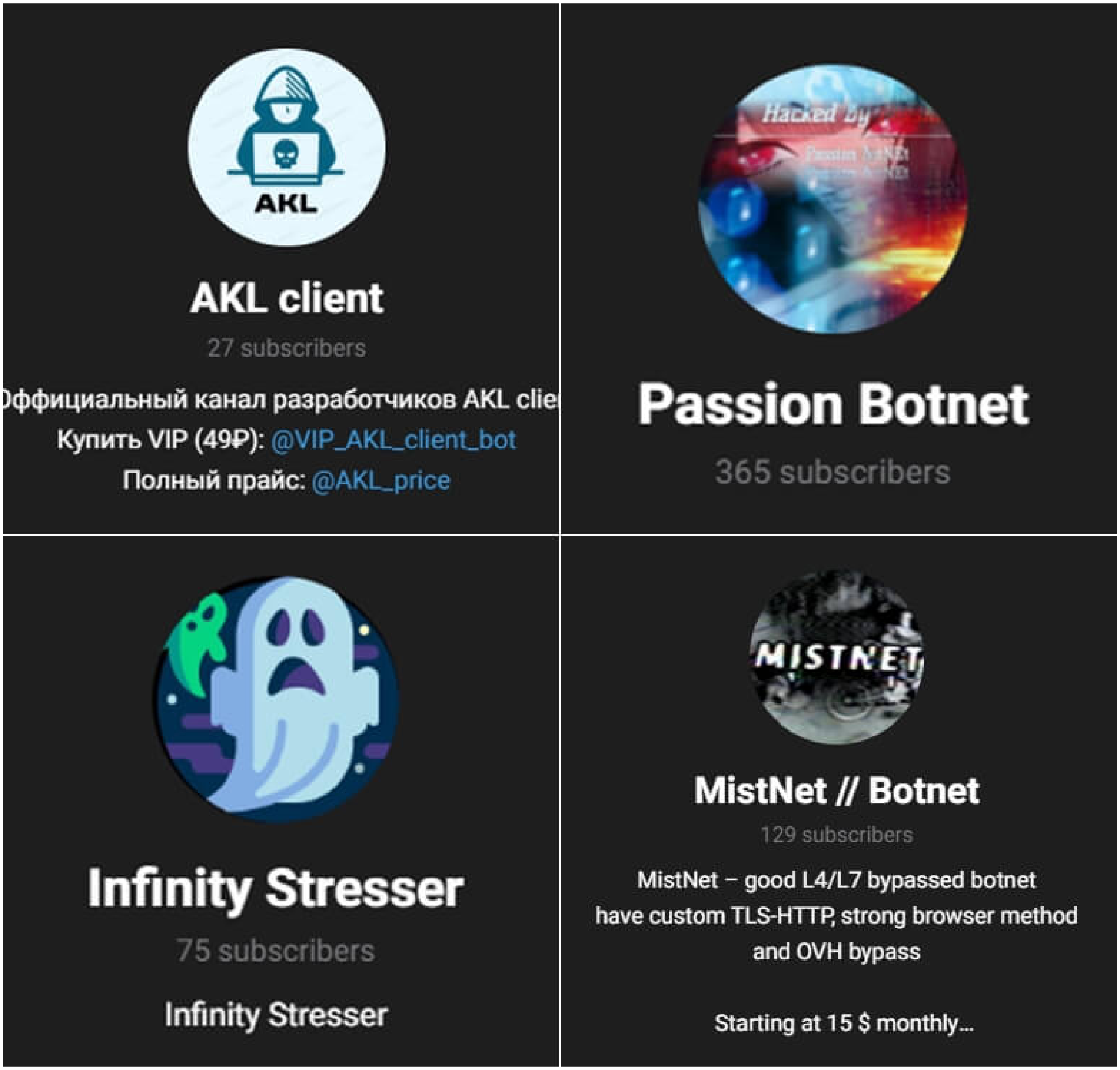
1 831 subscribers

Киберармия хактивистов и просто хороших людей

Глава новостей @MargoHARI
Глава IT @HagridRZ...

Killnet was recently observed operating with the Passion Botnet, a group that offers DDoS-as-a-Service. The origin of Passion is unknown, but they have become more active lately, especially at the beginning of 2023. They have a history of targeting individuals and organizations against Russia's invasion of Ukraine, using techniques like defacement and denial of service.

Also, other groups affiliated with Killnet offer DDoS as a Service model, such as AKL Client, Infinity Stresser, and MistNet.



AKL client

27 subscribers

ффициальный канал разработчиков AKL clie

Купить VIP (49₽): @VIP_AKL_client_bot

Полный прайс: @AKL_price

Passion Botnet

365 subscribers

Infinity Stresser

75 subscribers

Infinity Stresser

MistNet // Botnet

129 subscribers

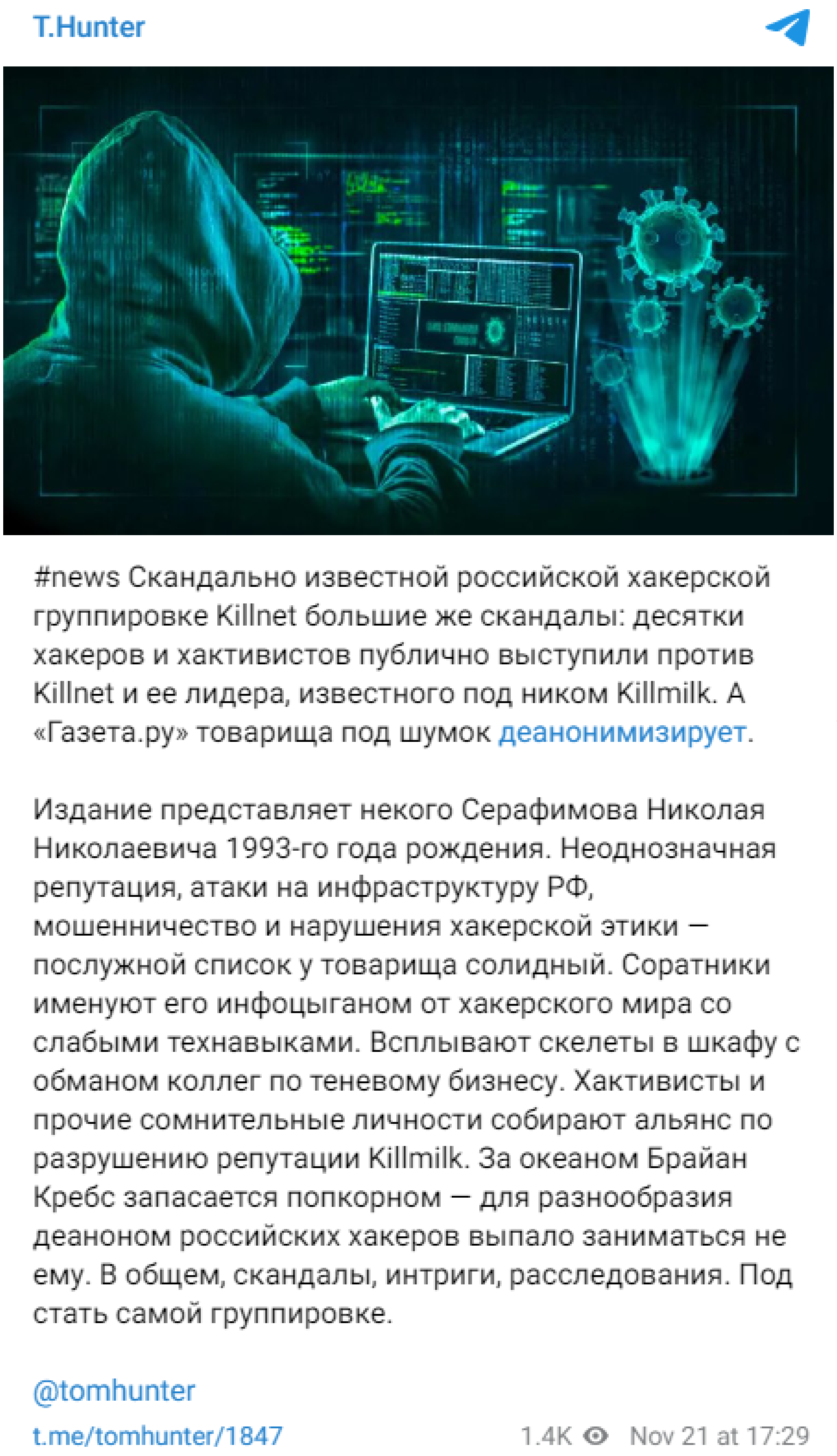
MistNet – good L4/L7 bypassed botnet
have custom TLS-HTTP, strong browser method
and OVH bypass

Starting at 15 $ monthly...

Killnet's cooperation with multiple DDos-as-a-Service providers may indicate that it will be more active in future events.

Unrest Within KillNet: Internal Conflict and Public Criticism

Recent developments indicate a significant internal rift within the notorious Russian hacktivist group KillNet. According to a Telegram post by a Russian-speaking researcher, dozens of hackers and hacktivists have publicly denounced KillNet and its leader, known by the alias KillMilk. Accusations of unethical behavior and inadequate technical skills against KillMilk mark this internal dissent.



#news Скандально известной российской хакерской группировке Killnet большие же скандалы: десятки хакеров и хактивистов публично выступили против Killnet и ее лидера, известного под ником Killmilk. А «Газета.ру» товарища под шумок деанонимизирует.

Издание представляет некого Серафимова Николая Николаевича 1993-го года рождения. Неоднозначная репутация, атаки на инфраструктуру РФ, мошенничество и нарушения хакерской этики — послужной список у товарища солидный. Соратники именуют его инфоцыганом от хакерского мира со слабыми технавыками. Всплывают скелеты в шкафу с обманом коллег по теневому бизнесу. Хактивисты и прочие сомнительные личности собирают альянс по разрушению репутации Killmilk. За океаном Брайан Кребс запасается попкорном — для разнообразия деаноном российских хакеров выпало заниматься не ему. В общем, скандалы, интриги, расследования. Под стать самой группировке.

@tomhunter
t.me/tomhunter/1847 1.4K Nov 21 at 17:29

Tom Hunter’s Telegram post, details explained below

In a deeper expose, Gazeta.ru has identified one person, Nikolai Nikolaevich Serafimov, born in 1993, as a key figure associated with KillMilk. Serafimov is described as having a contentious reputation, involving attacks against Russian infrastructure, fraudulent activities, and breaches of hacker ethics. His peers have labeled him as an “information gypsy” in the hacking world, offensively critiquing his limited technical prowess.

This internal turmoil within KillNet, marked by allegations and the potential de-anonymizing of its members, represents a significant chapter in the group's controversial existence, mirroring the very nature of the group itself.

Prominent Characteristics & TTPs

By observing Killnet's attacks and behavior to date, some inferences could be made about whether they are applied repetitively or consistently.

- Due to its motivation and determination to defend Russia, the group chose its targets among NATO-linked countries. It is also a potential threat to countries whose political interests contradict Russia.
- They prefer DDoS attacks against their targets. Victims can recover their systems from attacks, which usually take 1-3 days, with appropriate measures in a matter of hours.
- They target governments' or public institutions' websites. This way, they think that they signal to the victims that the victims chose the "wrong side."
- They announce their attacks and targets on Telegram channels.
- Killnet is also associated with other hacker groups that have common goals with them or act in Russian interests. They have been collaborating with XakNet and F**kNet, and the additional threat actors aforementioned.

MITRE Map

Reconnaissance	Resource Development	Credential Access	Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1110: Brute Force	T1498: Network Denial of Service
T1589: Gather Victim Identity Information	T1584: Compromise Infrastructure		T1489: Service Stop

Primary Killnet Tactics

Brute-force dictionary attacks against:

- SSH (port 22) primarily targets the root account
- Minecraft and TeamSpeak servers

DDoS attacks on the OSI model:

- layer 4 (SYN flood attacks)

- layer 7 (high volume POST/GET requests) to cause resource exhaustion and system failure.

In various Telegram groups, they collaborate with the members who are instructed to use IP stresser-for-hire tools such as Crypto Stresser, DDG Stresser, Instant-Stresser, and Stresser.ai. Moreover, several scripts are used during their attacks. Some of them are CC-attack, MDDoS, Low Orbit Ion Cannon (LOIC), KARMA, and Dummy.

How to Prevent a Killnet Attack

Firstly, we need to pay attention to two main defense tactics. One is enforcing strong password policies that can withstand basic brute-force credential attacks, and the second is to have a proper strategy for fighting off DDoS attacks.

The other defensive tactics are listed below:

- Purchase DDoS mitigation services from an Internet Service Provider (ISP), Content Delivery Network (CDN), or Web-Application Firewall (WAF) provider.
- Deploy multi-factor authentication (MFA) mechanism for all remote accesses
- Use blocklisting known Killnet-related IoC, such as IP addresses used by Killnet attacks.
- Enable the DMZ (Demilitarized Zone) for internet-facing entities.
- Employ DDoS protection via web bot detection techniques.
- Reduce attack surfaces and make it easier with ASM (Attack Surface Management) platforms.
- Get the CTI (cyber threat intelligence) feeds that monitor dark web information to identify and predict potential threats and provide actionable intelligence data for your organization.
- Configure web servers and APIs with security modules to optimize performance during a web traffic spike.
- Perform stress tests on all critical services for their ability to handle resource exhaustion attacks
- Create and practice IRP (Incident Response Plan) for the worst case, which resulted in temporary downtime.

Learn What Hackers Talk About Your Company With SOCRadar

The fact that **Telegram** is a legit messaging app used by millions gave hackers a chance to conceal themselves and follow their malicious agenda. More and more threat actors use Telegram for communication and announcements, and it has become the main hub for **threat actors**.