



ThreatMon



# IN-DEPTH ANALYSIS ON THE ROLES OF THREAT ACTORS AND ATTACKS IN THE UKRAINE-RUSSIA WAR

---

IT Army of UKRAINE



@threatmon



@MonThreat

<b>Summary</b>	<b>2</b>
<b>Cyber Wars in The Ukraine-Russia War</b>	<b>3</b>
<b>Threat Actor Review: IT Army of Ukraine</b>	<b>4</b>
Who is IT Army of Ukraine?	4
Which Side They Supports?	4
What Types of Attacks Does IT Army of Ukraine Execute?	4
Which Sectors Is IT Army of Ukraine Targeting?	6
<b>IT Army of Ukraine's Attacks</b>	<b>7</b>
Example attacks	7
October 24, 2022	7
December 22, 2022	8
February 28, 2022	9
January 16, 2023	10
January 25, 2023	10
February 15, 2023	11
February 20, 2023	12
February 24, 2023	12
March 1, 2023	13
March 15, 2023	15
March 20, 2023	16
March 25, 2023	17
<b>IT Army of Ukraine's Attack TTPs</b>	<b>18</b>
<b>IT Army of Ukraine's Attack IOCs</b>	<b>19</b>

## Summary

The beginning of the Russia-Ukraine war dates back to Russia's annexation of Crimea in 2014. The political tension that erupted in 2021-2022 was the last straw and Russian forces took action on Putin's orders. Taking action on February 24, 2022, Russian forces launched a large-scale invasion of Ukraine. Russian President Vladimir Putin claims that this is not an invasion, but that Russia is protecting its geopolitical interests in the region, its citizens and its deployed soldiers.

This report is the 4rd Report in a series of investigations on threat actors playing an active role in the Ukraine-Russia war, based on the IT Army of Ukraine report shared by ThreatMon earlier.

## Cyber Wars in The Ukraine-Russia War

In 2014, Russia annexed Crimea, leading to conflict in the Donbass region and the start of a cyber war between Ukraine and Russia. Since then, Ukraine has been a frequent target of Russian cyber attacks, including ransomware, DDoS, and data manipulation. These attacks have targeted critical sectors such as energy, finance, and communication.

One of the most notable cyber attacks on Ukraine occurred in 2015 when parts of the country experienced power cuts. The attack was allegedly carried out by the pro-Russian group Sandworm, which targeted the country's electricity grid. This cyber attack caused a worldwide debate on cybersecurity and served as a wake-up call for Ukraine to take stronger measures on cybersecurity.

Following the attack, Ukraine implemented several measures to enhance its cybersecurity capabilities. The country established a National Coordination Center for Cybersecurity and developed a national cybersecurity strategy. Additionally, the government introduced legislation to strengthen cybersecurity regulations and established partnerships with international organizations to share best practices and expertise.

Despite these efforts, Ukraine remains a target for cyber attacks from Russia. In 2017, the country was hit by another cyber attack, the NotPetya ransomware attack, which caused widespread disruption in Ukraine and other countries. The attack is believed to have been carried out by Russian hackers and caused billions of dollars in damage.

Ukraine's experience highlights the growing threat of cyber attacks and the need for countries to take cybersecurity seriously. As technology continues to advance, the risk of cyber attacks is only going to increase. Therefore, countries must continue to invest in cybersecurity measures to protect themselves from these threats.

## Threat Actor Review: IT Army of Ukraine

### Who is IT Army of Ukraine?

Two days after the Russian invasion, which started with Putin's announcement of a "special military intervention" on television on February 24, 2022, Ukraine's deputy prime minister and minister of digital transformation, Mykhailo Fedorov, announced the creation of a volunteer cyber army. Volunteers joining the group were divided into units to carry out DDoS attacks and the more experienced to perform complex cyber operations.

IT Army of Ukraine uses Twitter and Telegram channels to announce the attacks. A website has been created so that more volunteers can participate and the IT Army can install the tools it has developed, and the attacks and the consequences of their attacks are shared on Telegram channels.

### Which Side They Supports?

IT Army of Ukraine is a hacking group affiliated with Ukraine.

### What Types of Attacks Does IT Army of Ukraine Execute?

IT Army of Ukraine carries out DDoS (Denial-of-Service) attacks on the websites and networks they specify. These DDoS attacks sometimes happen to make a website completely unusable, and sometimes it happens to temporarily stop or slow down some systems to harm Russia's economy. As a result of these attacks, confidential information of the attacked systems is also leaked, and they share them in the Telegram group.

As we can see from the development of the situation surrounding the **dumps** received from the cbrf, they contain extremely sensitive information, as evidenced by the attempt by the ralist to block and delete the archives from the service <https://anonfiles.com/> In this regard, we have uploaded independent archives from each other of the above-mentioned dumps concerning military institutions and military personnel of the Russian Federation.

We don't stop there! There will be a lot more interesting information for you in the near future. Wait for announcements!

[https://anonfiles.com/F5laz3G8y7/67\\_rar](https://anonfiles.com/F5laz3G8y7/67_rar) 18.18 GB  
[https://anonfiles.com/F8oez0G6yc/68\\_rar](https://anonfiles.com/F8oez0G6yc/68_rar) 10.75 GB  
[https://anonfiles.com/y9r2zcG7yf/69\\_rar](https://anonfiles.com/y9r2zcG7yf/69_rar) 14.3 GB

They support these attacks with tools they wrote themselves or with open source proxies such as "Death By 1000 Needles" or "mhhddos\_proxy".

The screenshot shows a Windows application window titled "UkITA Installer Setup". The main title bar says "UkITA Installer Setup". The window content is titled "Telegram ID" with the sub-instruction "Add a personal Telegram Bot identifier". On the right side of the window, there is a logo featuring a shield with the letters "IT" and a blue and yellow striped background. Below the title, a message states: "Our new Telegram bot has learned to provide the personal ID of a participant in a ddos attack." A blue link "https://t.me/itarmy\_stat\_bot" is provided. Below this, another message says: "And if you run the ddos utility with the ID, the bot will easily provide informative personal statistics..". A red arrow points from the text "More details on the website:" to the link "https://itarmy.com.ua/statistics". Another red arrow points from the text "Add identifier" to the input field containing the value "9379992". At the bottom of the window, there are three buttons: "< Back", "Install", and "Cancel".

The screenshot shows a web browser displaying the "IT Army of Ukraine" website. The URL is "https://itarmy.com.ua". The page title is "UKRAINE IT ARMY INSTALLER FOR WINDOWS (ALL IN ONE - MHDDOS/DB1000N/DISTRESS)". The page content includes a brief description: "You can contact for help at [IT Army of Ukraine Chat](#). Download and install - [UkITA Installer](#) ([https://github.com/OleksandrBlack/ukita\\_installer](https://github.com/OleksandrBlack/ukita_installer)) Visualization of the installation and launch of the attack". Below this, there is a large "IT Army of Ukraine" logo featuring a shield with "IT" and a gear. The left sidebar of the website has links like "Home", "Start DDOS info", "VPS info (UA)", "Partners", "Automated bot", "Statistics", and "Наш телеграм канал".

## Which Sectors Is IT Army of Ukraine Targeting?

IT Army Of Ukraine has targeted almost all sectors in the last year. In total, it has carried out DDoS attacks by sharing over 9,100 individual IP addresses and URLs on the Telegram channel. In order from most to least:

- Government-run Websites (Courts, Ministry Of Foreign Affairs, Post Office, Russian Parliament, Beverage Delivery Service...)
- Bank, Payment Systems And Stock Market (Qiwi, Gazprom Bank, Central Bank, Paytrans, Alfa-bank, Moex, Sberbank...)
- Media (Mk.ru, Gazeta.ru, Aif.ru, Tass.ru...)
- Propaganda Websites
- Auction Sites (Rosltorg)
- Television Channels And Services (Okko.tv, Wink.ru)
- Video Conferencing Apps/sites
- Logistics (Ati.su, Datrans.ru, Dellin.ru)
- Audit And Accounting Services
- Sites Selling Military Equipment (Voentorg, 2gis)
- Websites Of Terrorist Groups Against Ukraine
- Ticket Reservation Sites (Booking Website)
- Websites Selling Unmanned Aerial Vehicles (Copter Drone Shops, Citilink.ru)
- University Websites
- Insurance Companies
- Holdings
- Courier Services (Express.dhl.ru, Boxberry.ru)
- Cinema And Tv Series Services
- Telecom And Communication Companies (Crelcom.ru)
- Internet Service Providers (Farline.net, Miranda-media, Dom.ru)
- Airlines
- Food Delivery Sites (Vkusvill.ru, Smokat.ru, Utkonos.ru)
- Electronic And E-commerce Sites (Wildberries.ru, Ozon.ru, Chipdip.ru)
- Veterinarians (Vetis)
- Petrol And Gas Trading Sites
- Freelance Platforms (Fl.ru, Advego.com)
- Job Sites (Superjob, Hh.ru, Zarplata.ru)
- Ddos Guards
- Automotive Industry (Drom.ru, Exist.ru, Autodoc.ru)
- Importer Companies (Dns-shop.ru)
- Search Engines

Many other industries have been the target of these attacks.

# IT Army of Ukraine's Attacks

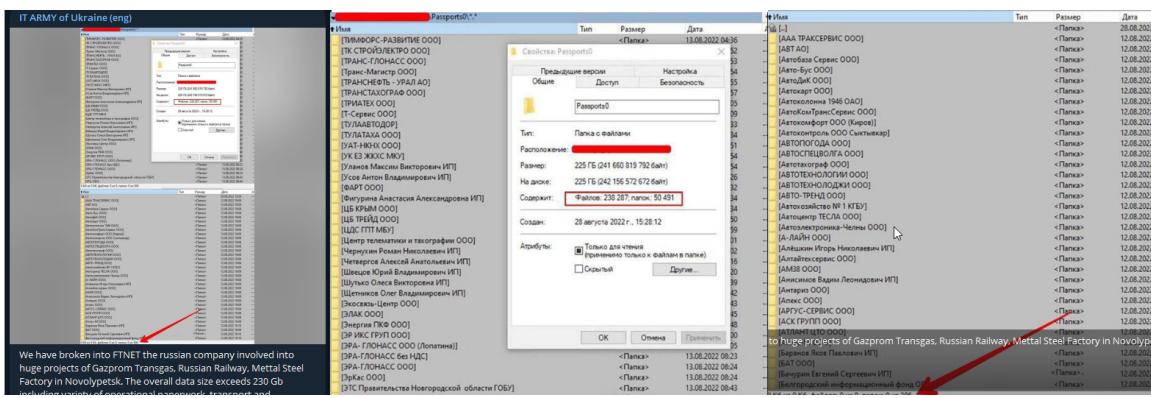
Here are some examples of cyber attacks involving IT Army of Ukraine directly or indirectly:

## Example attacks

October 24, 2022

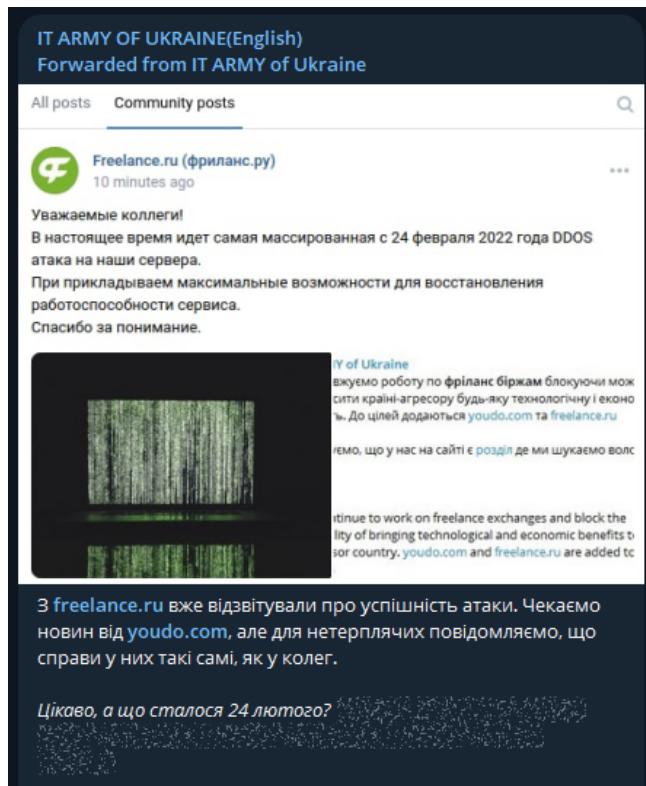
On October 24, 2022, the IT ARMY of Ukraine group accessed and extracted more than 230 Gb of large databases of its victims. This data included various operational documents, transportation and employee profiles.

Gazprom Transgaz, Russian Railways, Mettal Steel Plant in Novolypetsk, Russian company FTNET



December 22, 2022

On December 22, 2022, the IT ARMY OF UKRAINE group was behind the attack on Russian-affiliated freelance.ru. With DDoS attacks, they forced the victim to remain offline for a certain period of time.



February 28, 2022

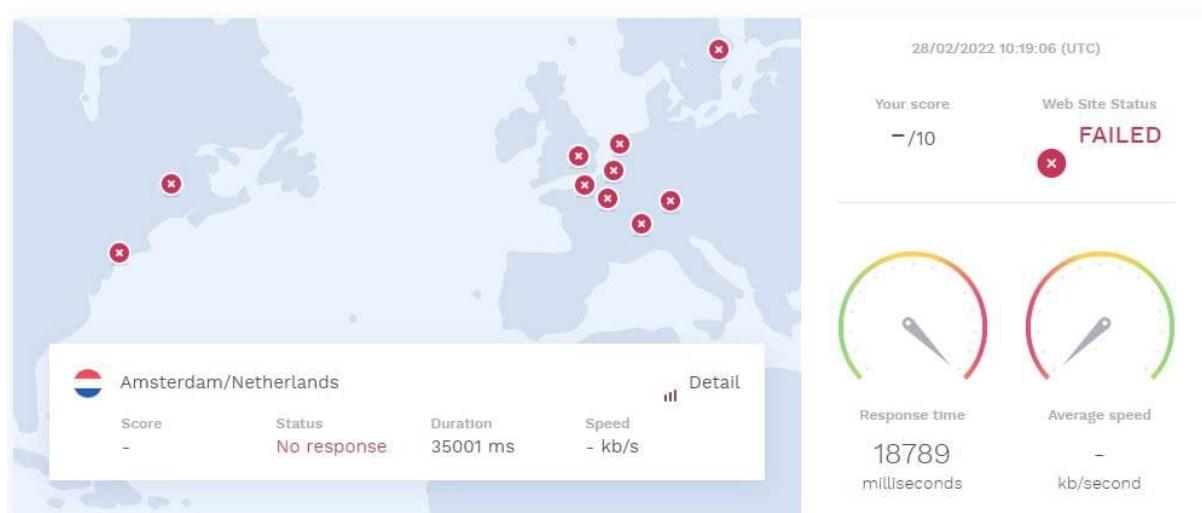
On February 28, 2022, Sberbank main domain and many ATMs became unusable due to DDOS attacks on Sberbank DNS servers.

### IT ARMY of Ukraine

На даний момент люди в РФ масово знімають кошти з банкоматів. Ми можемо завдати колосальний урон вдаривши по DNS сбербанку!

Наша ціль [www.sberbank.ru](https://www.sberbank.ru)

53 UDP  
53 UDP  
53 UDP  
53 UDP



## January 16, 2023

January 16, 2023 After the attack on the Russian Regional Development Bank, they caused the fuel cards to not work at the gas stations.

### IT ARMY OF UKRAINE(English) Forwarded from IT ARMY of Ukraine



### На многих заправках в Башкирии стало проблемой расплатиться картами

Причина может быть на стороне подсанкционного банка ВБРР - партнера «Роснефти».

(10 января 2023 09:31 , ИА "Девон" )

В Башкирии на автозаправках «Башнефти» (группа «Роснефть») с 9 января отмечены сбои при оплате безналичным способом. Страдают как обычные автовладельцы, так и организации. Например, водителей скорой помощи предупредили о возможных перебоях при оплате топливными картами и предложено в таких случаях платить наличными с сохранением чеков. Об этом сообщило издание UFA1.RU.

На горячей линии «Башнефти» сообщили, что проблема уже устранена на части АЗС, но на некоторых заправочных станциях всё еще могут наблюдаться сбои.

## January 25, 2023

Owned by Russia on January 25, 2023 They targeted digital accounting firm Sbis.

### IT ARMY OF UKRAINE(English) Forwarded from IT ARMY of Ukraine

The screenshot shows a blog post titled "DDoS-атаки 24 января 2023 г." (DDoS attacks on January 24, 2023). The post discusses a DDoS attack on January 24, 2023, targeting the fiscal digital accounting system (FDS) of Russia. It states that access to personal cabinets was interrupted due to technical issues, but data transmission between the FDS and its clients remained stable. The post also provides contact information for urgent communication via online chat or a bot.

Новости

Обновления продуктов

Цифры и кейсы

Видеоролики

Инструкции

Обзоры продуктов

Вебинары

Уважаемые клиенты и партнеры!

С 11:50 24 января 2023 г. на ресурсы операторов фискальных данных России и производителей ККТ осуществляются DDoS-атаки.

В настоящее время доступы в личные кабинеты работают с перебоями, но работоспособность всех сервисов восстановлена.

Передача данных в ФНС осуществляется в штатном режиме. Ваши персональные и коммерческие данные были и остаются надежно защищены.

Для срочной связи с нами вы можете воспользоваться онлайн-чатом или чат-ботом

Троїцімо економічний сектор болотян далі! До поточних цілей додали офд сервіс від [Сбіс](#).

February 15, 2023

February 15, 2023 They gained access to the corporate network of PayTrans, an IT company that serves the payments of Moscow's normal and medium-capacity metro. It leaked source code for online payment mobile apps, application server for wire transfers, ORA2 and ORA1 for payment transactions, CCTV data.

```
Powering off VM:  
Power off failed  
[root@esxi:] vim-cmd vmsvc/power.off 22  
Powering off VM:  
Power off failed  
[root@esxi:] rm -f /vmfs/volumes/datastore0/*  
.fbb.sf vm_alpha_clone/  
.fdc.sf vm_beta/  
.jbc.sf vm_bk/  
.locker/ vm_confluence/  
.pb2.sf vm_delta/  
.pho.sf vm_first_test/  
.sbc.sf vm_for_test_new_apb/  
.sdd.sf/ vm_gamma/  
.vh.sf vm_jira/  
.iso/ vm_minpromptorg/  
vm_ASU_PBK/ vm_mm_suv_kitchen_clone/  
vm AlpineLinux docker/ vm_nvr/  
vm_MM_automdownload_win2003r2ru/ vm_vipnet/  
vm_win2003_MM_certcenter/ vm_win2012_20191021/  
vm_alpha/- vm_winprog/  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_ASU_PBK/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_AlpineLinux_docker/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_MM_automdownload_win2003r2ru/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_Win2003_MM_certcenter/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_alpha/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_alpha_clone/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_beta/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_bk/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_delta/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_first_test/*  
rm: can't remove '/vmfs/volumes/datastore0/vm_first_test/vm_first_test-000001-sesparse.vmdk': Device or resource busy  
rm: can't remove '/vmfs/volumes/datastore0/vm_first_test/vm_first_test-28425ald.vsp': Device or resource busy  
rm: can't remove '/vmfs/volumes/datastore0/vm_first_test/vm_first_test-flat.vmdk': Device or resource busy  
rm: can't remove '/vmfs/volumes/datastore0/vm_first_test/vm_first_test.vmx.lock': Device or resource busy  
rm: can't remove '/vmfs/volumes/datastore0/vm_first_test/vmx-vm_first_test-675437085-1.vsp': Device or resource busy  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_for_test_new_apb/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_gamma/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_jira/*  
[root@esxi:] rm -f /vmfs/volumes/datastore0/vm_minpromptorg/*  
rm: can't remove '/vmfs/volumes/datastore0/vm_minpromptorg/ca46ddb4.vsp': Device or resource busy  
rm: can't remove '/vmfs/volumes/datastore0/vm_minpromptorg/vm_minpromptorg-flat.vmdk': Device or resource busy  
rm: can't remove '/vmfs/volumes/datastore0/vm_minpromptorg/vm_minpromptorg.vmx.lock': Device or resource busy
```

Метро Москвы – метро, МЦД, МЦК

Оценки и отзывы

Вам помогла эта информация? Да Нет

ТЫКВЕННОЕ\_ВАРЕНЬЕ 8 февраля 2023 г.

После последних обновлений приложение отказывается показывать мои карты и данные! В приложении висит значок ошибки... Уже несколько раз удалял приложение и устанавливал его заново, и только после этого оно начинает работать несколько дней, а потом всё опять повторяется!

Вам помогла эта информация? Да Нет

Михаил Телепнев 7 февраля 2023 г.

Полностью перестал работать доступ к картам и пополнениям, приложение стало бесполезным, АЖАЛЬ. Пробовал чистить каш, данные на телефоне, физические следы в виде файлов, переустанавливал, повторял несколько раз. Все бесполезно!

1 человек отметил этот отзыв как полезный.

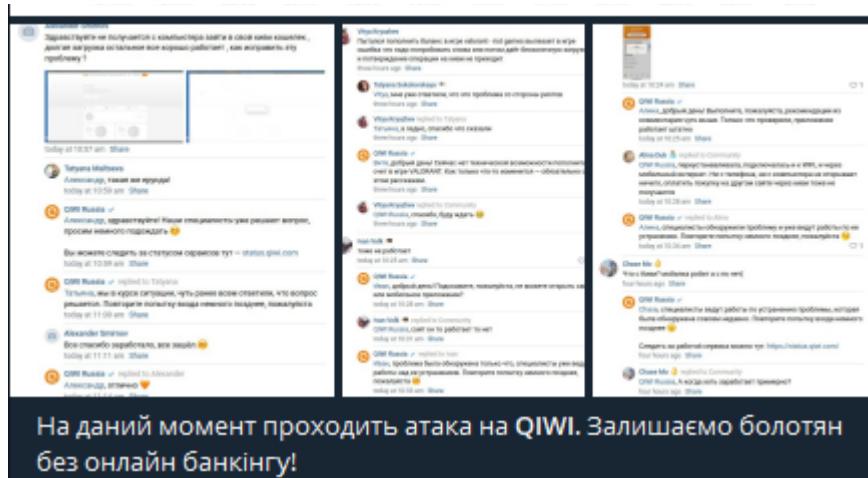
Вам помогла эта информация? Да Нет

Наталья Сашина

Активизирована 2023 год

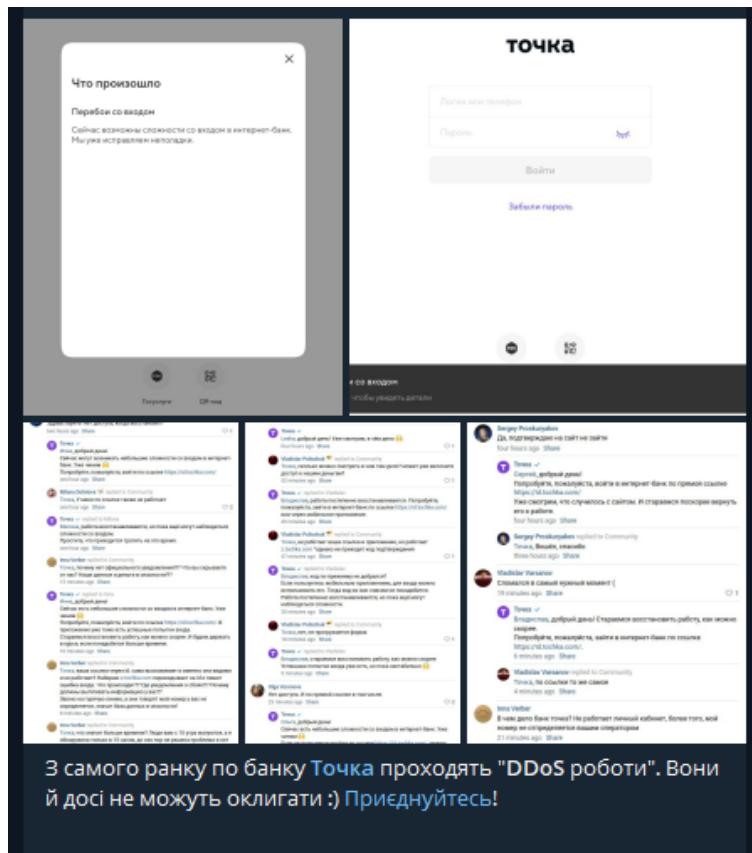
February 20, 2023

February 20, 2023 QIWI Bank, headquartered in Cyprus, suffered a cyber attack that damaged its reputation with its customers.



February 24, 2023

IT ARMY OF UKRAINE February 24, 2023 The Russian digital bank blocked its operations as a result of a DDoS attack against Tochka.



March 1, 2023

March 1, 2023 IT ARMY OF UKRAINE carried out a successful DDoS attack on Russian customs, leading to a system failure in the electronic declaration process and blocking the cargo customs clearance procedure.

The screenshot shows a news article from SecurityLab.ru. The title is "Федеральная таможенная служба подверглась DDoS-атаке" (Russia's customs service suffered a DDoS attack). The article discusses how the Federal Customs Service (FTC) reported a DDoS attack on its information systems, which disrupted the electronic declaration process and cargo clearance. The attack was described as unprecedented. The article includes a link to The Moscow Times article and a statement from the FTC.

**IT ARMY OF UKRAINE(English)**  
Forwarded from IT ARMY of Ukraine

**SecurityLab.ru**  
by Positive Technologies

**Федеральная таможенная служба подверглась DDoS-атаке**

241 / 28 февраля, 2023

DDoS-атака | ФТС | Альта-Софт | таможня

сколько часов растаможка грузов была невозможна.

Федеральная таможенная служба (ФТС) в своем Telegram-канале сообщила о DDoS-атаке, которая произошла утром 28 февраля. По данным ФТС, проблема была решена, и работа ресурсов ФТС не прервана. В то же время атаки отразились на работе информоператоров, передающих информацию в таможенные органы.

Правительство также отметило, что система электронного сканирования товаров «Альта-Софт» 28 февраля подверглась «беспрецедентной кибератаке», которая нарушила процессы стаможивания грузов. Систему «Альта-Софт» является одной из многих используемых для подачи данных в таможенную службу.

Утром 28 февраля «Альта-Софт» разослала клиентам уведомление о «войне DDoS-атаке», которая началась в 8:10 утра и длилась сколько часов. Кибератака привела к сбою в системе электронного сканирования. В этот же день в 13:00 специалисты компании полностью восстановили обмен данными с таможенными органами.

**Вчора ми успішно здійснили не анонсовану DDoS-атаку на росіянську митницю, що призвело до збоїв у системі електронного декларування та до блокування розмитнення вантажів!**

**IT-системы российской таможни рухнули после «беспрецедентной кибератаки»**

Сообщение о том, что правительство России заявило о блокировке информационных систем таможни и электронной таможни, нарушении функционирования информационных систем таможни и электронной таможни, а также о том, что были предприняты меры по восстановлению работы, было опубликовано в среду, 28 февраля.

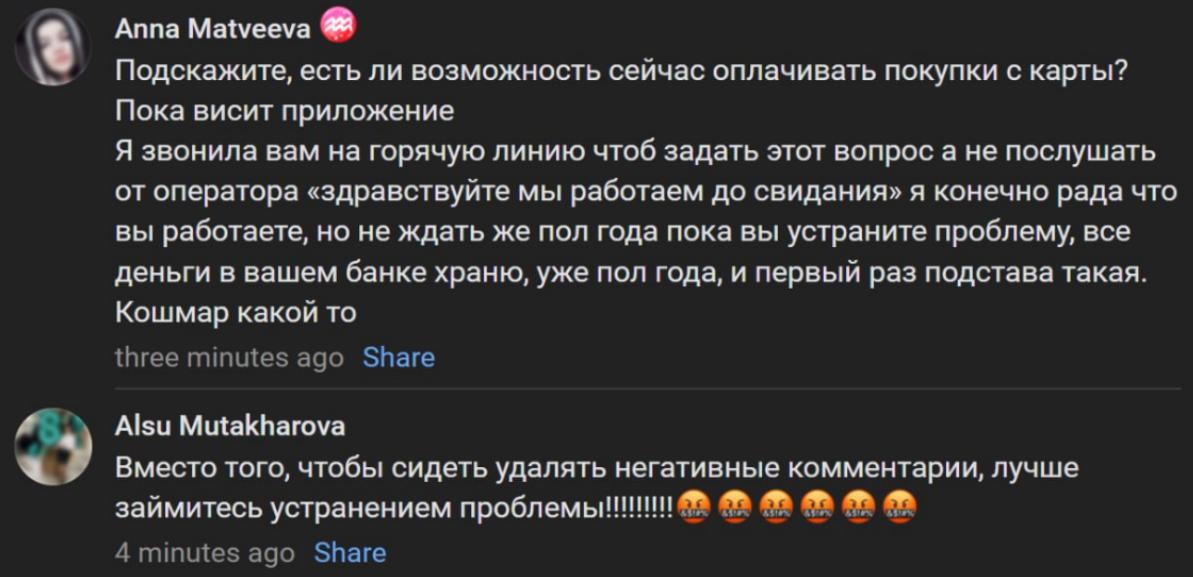
Сообщение о том, что правительство России заявило о блокировке информационных систем таможни и электронной таможни, а также о том, что были предприняты меры по восстановлению работы, было опубликовано в среду, 28 февраля.

Сообщение о том, что правительство России заявило о блокировке информационных систем таможни и электронной таможни, а также о том, что были предприняты меры по восстановлению работы, было опубликовано в среду, 28 февраля.

Сообщение о том, что правительство России заявило о блокировке информационных систем таможни и электронной таможни, а также о том, что были предприняты меры по восстановлению работы, было опубликовано в среду, 28 февраля.

March 15, 2023

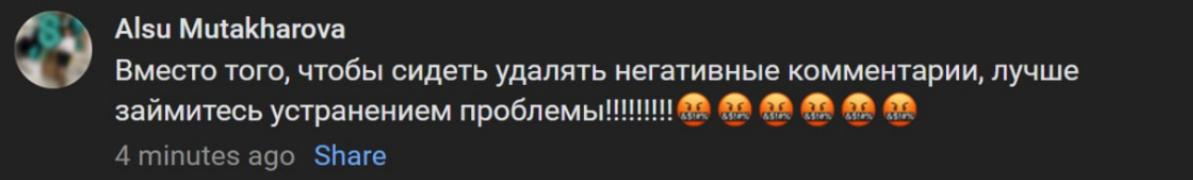
On March 15, 2023, the targeted Bank Bars fell victim to DDoS and lost many of its customers. So the IT ARMY OF UKRAINE group got what it wanted.



Anna Matveeva  Подскажите, есть ли возможность сейчас оплачивать покупки с карты? Пока висит приложение Я звонила вам на горячую линию чтобы задать этот вопрос а не послушать от оператора «здравствуйте мы работаем до свидания» я конечно рада что вы работаете, но не ждать же пол года пока вы устраниете проблему, все деньги в вашем банке храню, уже пол года, и первый раз подстава такая. Кошмар какой то

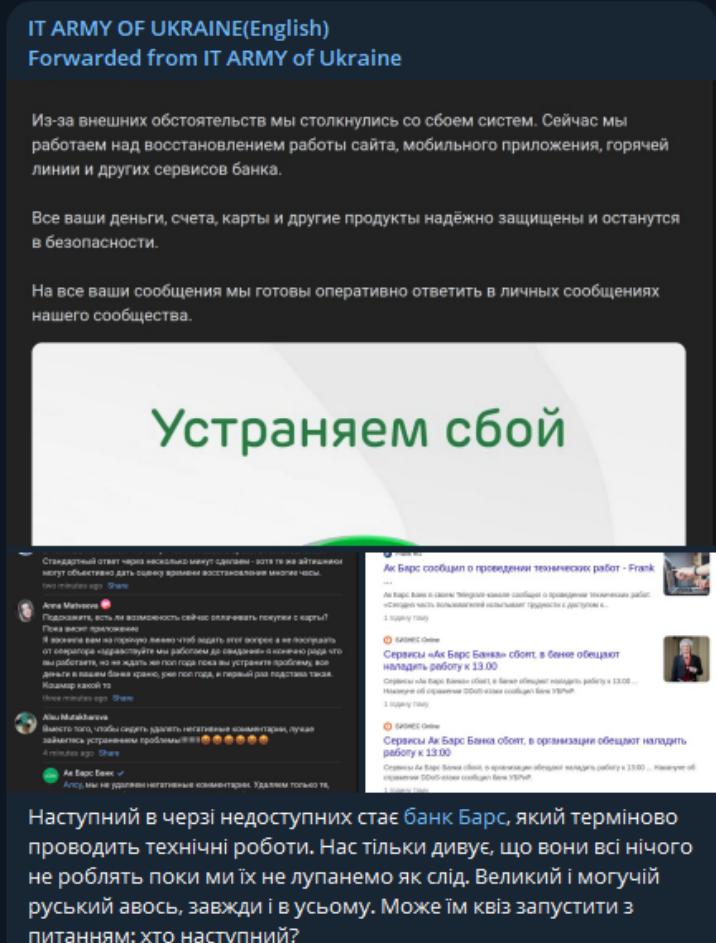
three minutes ago Share

---



Alsu Mutakharova Вместо того, чтобы сидеть удалять негативные комментарии, лучше займитесь устранением проблемы!!!!!!!!!! 

4 minutes ago Share

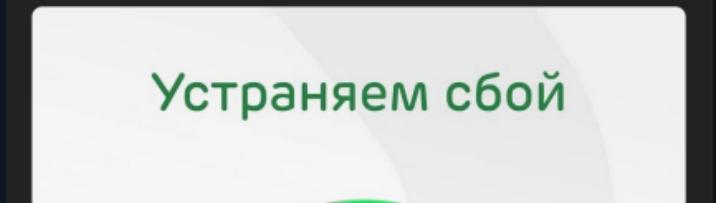


IT ARMY OF UKRAINE(English)  
Forwarded from IT ARMY of Ukraine

Из-за внешних обстоятельств мы столкнулись со сбоем систем. Сейчас мы работаем над восстановлением работы сайта, мобильного приложения, горячей линии и других сервисов банка.

Все ваши деньги, счета, карты и другие продукты надежно защищены и останутся в безопасности.

На все ваши сообщения мы готовы оперативно ответить в личных сообщениях нашего сообщества.



## Устранием сбой

Стандартный ответ через несколько минут сделаны - хотя те же айтишники могут объективно дать оценку времени восстановления многих часов.

two minutes ago Share

Anna Matveeva  Подскажите, есть ли возможность сейчас оплачивать покупки с карты? Пока висит приложение Я звонила вам на горячую линию чтобы задать этот вопрос а не послушать от оператора «здравствуйте мы работаем до свидания» я конечно рада что вы работаете, но не ждать же пол года пока вы устраниете проблему, все деньги в вашем банке храню, уже пол года, и первый раз подстава такая. Кошмар какой то

three minutes ago Share

Alsu Mutakharova  Вместо того, чтобы сидеть удалять негативные комментарии, лучше займитесь устранением проблемы!!!!!! 

4 minutes ago Share

Ак Барс  Ак Барс сообщает о проведении технических работ - Frank 

Ак Барс в связи с текущими заявками сообщает о проведении технических работ. «Следует часть пользователей испытывать трудности с доступом к...»

1 minute ago

ОБНОВЛЕНИЕ Сервисы Ак Барс Банка сбоят, в банке обещают наладить работу к 13:00 ... Службы Ак Барс Банка сбоят, в банке обещают наладить работу к 13:00 ... Наконец обновление DDoS атаки подстерегает банк ТРКНТ.

1 minute ago

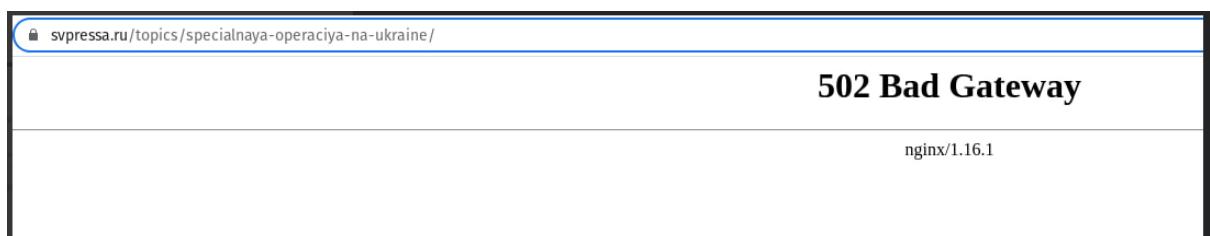
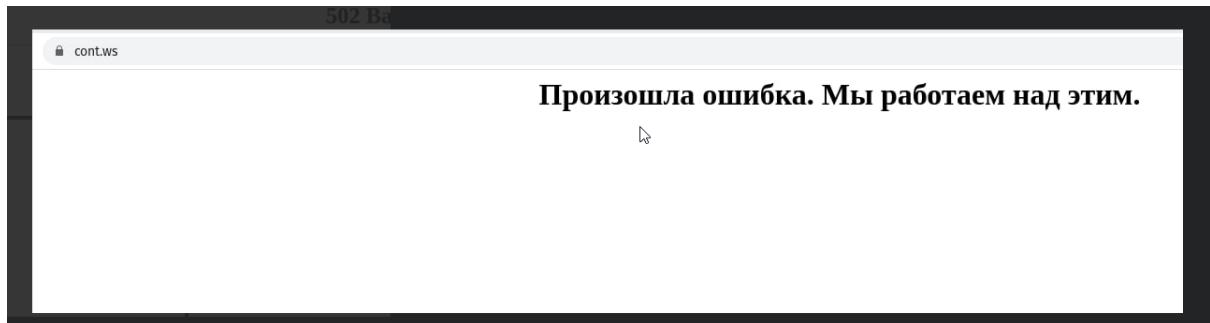
ОБНОВЛЕНИЕ Сервисы Ак Барс Банка сбоят, в организации обещают наладить работу к 13:00 ... Сервисы Ак Барс Банка сбоят, в организации обещают наладить работу к 13:00 ... Наконец обновление DDoS атаки подстерегает банк ТРКНТ.

1 minute ago

Наступний в чергі недоступних стає банк Барс, який терміново проводить технічні роботи. Нас тільки дивує, що вони всі нічого не роблять поки ми їх не лупанемо як слід. Великий і могучий руський авось, завжди і в усьому. Може їм квіз запустити з питанням: хто наступний?

March 20, 2023

On March 20, 2023, the banking system "ABR Bank" fell victim to a DDoS attack that interrupted all its operations.



IT ARMY OF UKRAINE(English)  
Forwarded from IT ARMY of Ukraine

Произошла ошибка. Мы работаем над этим.

svpressa.ru/topics/specialnaya-operaciya-na-ukraine/

502 Bad Gateway

nginx/1.16.1

cont.ws

Svpressa

svpressa.ru

На вихідних банківських поширилася на банк Росія. Символично, після купії регіональних назв ми поклали усю "Расію", правда? А також додали трошки інформаційної гігієни відключивши купу новинних помийок. Вікенд вдається.

ABR.ru не работает сегодня Март 2023?  
Последний раз было открыто соединение 18 марта 2023 года  
Изменить веб-страницу: ABR.ru веб-страница последний 24 часа

Город	Количество
Москва	5
Санкт-Петербург	4
Тверь, Тверская область	3
Ростов, Ростовская область	2
Севастополь, Советскоград	2
Санкт-Петербургский край	2
Волгоград, Волгоградская область	1
Кострома, Костромская область	1
Нижний Новгород	1

March 25, 2023

On March 25, 2023, IT ARMY has been silent for a few days, but during this period, they launched DDoS attacks on two important banks belonging to Russia, Novikom and Russian Agrarian Bank, rendering them unusable for a certain period of time.

The screenshot shows a news article from 'IT ARMY OF UKRAINE(English)' with the subtitle 'Forwarded from IT ARMY of Ukraine'. The article discusses the website Novikom.ru experiencing downtime. It includes a screenshot of a forum post where users report being unable to log in to the PCXБ app or website. Another screenshot shows a live chat interface with a user asking about service availability. Below these are two charts showing website traffic and connection errors over a 24-hour period. The text at the bottom of the page discusses the impact of such outages on Ukrainian companies.



## IT Army of Ukraine's Attack TTPs

Tactics	Technique	Technique ID
Impact	Endpoint Denial of Service: Service Exhaustion Flood	T1499.002
Impact	Network Denial of Service: Direct Network Flood	T1498.001
Reconnaissance	Active Scanning: Scanning IP Block	T1595.001
Reconnaissance	Gather Victim Network Information: DNS	T1590.002
Reconnaissance	Gather Victim Network Information: IP Addresses	T1590.005
Collection	Data From Local System	T1005

## IT Army of Ukraine's Attack IOCs

IOC	IOC Type
xn--80aafyzixh[.]xn--j1amh	Domain
<a href="http://www[.]zdg[.]md">www[.]zdg[.]md</a>	Domain
<a href="http://www[.]usatoday[.]com/search/results?q=">www[.]usatoday[.]com/search/results?q=</a>	Domain
<a href="http://www[.]ukrinform[.]ru">www[.]ukrinform[.]ru</a>	Domain
<a href="http://www[.]ted[.]com/search?q=">www[.]ted[.]com/search?q=</a>	Domain
<a href="http://www[.]stily[.]ge">www[.]stily[.]ge</a>	Domain
<a href="http://www[.]rondevo[.]com">www[.]rondevo[.]com</a>	Domain
<a href="http://www[.]psichopatas[.]lt">www[.]psichopatas[.]lt</a>	Domain
<a href="http://www[.]picuki[.]com">www[.]picuki[.]com</a>	Domain
<a href="http://www[.]ostro[.]org">www[.]ostro[.]org</a>	Domain
<a href="http://www[.]onlinedics[.]ru">www[.]onlinedics[.]ru</a>	Domain
<a href="http://www[.]mamywiekszego[.]pl">www[.]mamywiekszego[.]pl</a>	Domain
<a href="http://www[.]fbi[.]com">www[.]fbi[.]com</a>	Domain
<a href="http://www[.]dynamomania[.]com">www[.]dynamomania[.]com</a>	Domain
<a href="http://www[.]cia[.]gov/index[.]html">www[.]cia[.]gov/index[.]html</a>	Domain
<a href="http://www[.]bigmir[.]net">www[.]bigmir[.]net</a>	Domain
<a href="http://www[.]jalia[.]ge">www[.]jalia[.]ge</a>	Domain
<a href="http://www[.]abw[.]by">www[.]abw[.]by</a>	Domain
<a href="http://www[.]1variant[.]ru">www[.]1variant[.]ru</a>	Domain
<a href="http://war[.]lt">war[.]lt</a>	Domain
<a href="http://vug[.]pl/takeRussiaDown[.]html">vug[.]pl/takeRussiaDown[.]html</a>	Domain
<a href="http://vug[.]pl">vug[.]pl</a>	Domain
<a href="http://vtemu[.]by">vtemu[.]by</a>	Domain
<a href="http://vlast[.]kz">vlast[.]kz</a>	Domain
<a href="http://v3[.]jrmk[.]net">v3[.]jrmk[.]net</a>	Domain
<a href="http://ukrainiancharm[.]com">ukrainiancharm[.]com</a>	Domain
<a href="http://ukraine[.]is-great[.]org">ukraine[.]is-great[.]org</a>	Domain
<a href="http://ua[.]korrespondent[.]net">ua[.]korrespondent[.]net</a>	Domain
<a href="http://tv8[.]md">tv8[.]md</a>	Domain
<a href="http://trendy-u[.]com">trendy-u[.]com</a>	Domain
the-list[.]ams3[.]cdn[.]digitaloceanspaces[.]com omtarahtino[.]notion[.]site/tarahtino	Domain

<a href="#">talkytimes[.]com</a>	Domain
<a href="#">talkyminute[.]com</a>	Domain
<a href="#">talkyhour[.]com</a>	Domain
stoprussianweb[.]eu	Domain
<a href="#">stopputin[.]ddns[.]net</a>	Domain
stop-russian-fake[.]news	Domain
<a href="#">stop-russia[.]synergize[.]co</a>	Domain
<a href="#">stop-russia[.]rf[.]gd</a>	Domain
<a href="#">stop-russia[.]great-site[.]net</a>	Domain
stop--russian--desinformation-near-page[.]translate[.]goog	Domain
<a href="#">stiri[.]md</a>	Domain
<a href="#">star[.]korupciya[.]com</a>	Domain
slavaukraini[.]online	Domain
<a href="#">slavaukraini[.]000webhostapp[.]com</a>	Domain
<a href="#">sbiblio[.]com</a>	Domain
russianwarshipgofuckyourself[.]club	Domain
russia-must-be-stopped-6mpfu[.]ondigitalocean[.]app	Domain
<a href="#">ru[.]jooble[.]org</a>	Domain
<a href="#">romancetale[.]com</a>	Domain
<a href="#">ringside24[.]com</a>	Domain
realist[.]online	Domain
raid[.]shell[.]enes[.]tech	Domain
<a href="#">rf[.]search[.]yahoo[.]com</a>	Domain
<a href="#">putler[.]whonnock[.]sk</a>	Domain
putin-huilo[.]xyz	Domain
<a href="#">primetime[.]ge</a>	Domain
<a href="#">pravdatutnews[.]com</a>	Domain
<a href="#">point[.]md</a>	Domain
play[.]tavr[.]media	Domain
<a href="#">pia[.]ge</a>	Domain
<a href="#">peliskovi[.]cz</a>	Domain
peimquizpol[.]xyz/	Domain
<a href="#">padaread[.]com</a>	Domain

<a href="#">padabum[.]com</a>	Domain
ovh1[.]vanagas[.]tech	Domain
osvita[.]name	Domain
omore[.]city	Domain
<a href="#">officiel-online[.]com</a>	Domain
nowar[.]1plus[.]red	Domain
<a href="#">norussian[.]tk</a>	Domain
<a href="#">news[.]bigmir[.]net</a>	Domain
<a href="#">neagent[.]by</a>	Domain
<a href="#">mw1[.]vdl[.]pl</a>	Domain
<a href="#">megatv[.]ge</a>	Domain
<a href="#">mbox[.]bigmir[.]net</a>	Domain
<a href="#">mamywiekszego[.]pl</a>	Domain
<a href="#">m[.]valentime[.]com</a>	Domain
<a href="#">m[.]rondevo[.]com</a>	Domain
<a href="#">m[.]orchidromance[.]com</a>	Domain
<a href="#">m[.]loveswans[.]com</a>	Domain
<a href="#">m[.]funchatt[.]com</a>	Domain
<a href="#">m[.]derzhava-sveta[.]webnode[.]ru</a>	Domain
<a href="#">m[.]amourfeel[.]com</a>	Domain
<a href="#">m[.]amourfactory[.]com</a>	Domain
<a href="#">m[.]999[.]md</a>	Domain
<a href="#">livebeam[.]com</a>	Domain
<a href="#">lady[.]tochka[.]net</a>	Domain
<a href="#">kuzelovi[.]cz</a>	Domain
<a href="#">kratkoe[.]com</a>	Domain
<a href="#">korupciya[.]com</a>	Domain
<a href="#">korrespondent[.]net</a>	Domain
<a href="#">konspiracie[.]torsk[.]sk</a>	Domain
<a href="#">knizhnik[.]org</a>	Domain
<a href="#">kinowar[.]com</a>	Domain
<a href="#">kaszaniok[.]github[.]io</a>	Domain
<a href="#">kanalukraina[.]tv</a>	Domain
<a href="#">joinposter[.]com</a>	Domain
<a href="#">jebacruskich[.]page</a>	Domain

<a href="#">ipfs[.]io</a>	Domain
<a href="#">internetua[.]com</a>	Domain
higherror[.]notion[.]site	Domain
help-ukraine-win[.]web[.]app	Domain
<a href="#">help-ukraine-win[.]s3[.]eu-west-1[.]amazonaws[.]com/index[.]html</a>	Domain
<a href="#">help-ukraine-win[.]s3[.]eu-west-1[.]amazonaws[.]com</a>	Domain
<a href="#">help-ukraine-win[.]firebaseapp[.]com</a>	Domain
gonzo[.]shell[.]enes[.]tech	Domain
<a href="#">glavpost[.]com</a>	Domain
<a href="#">github[.]com/chmod777anarchy</a>	Domain
<a href="#">gazetaby[.]com</a>	Domain
fuck-desinformation[.]netlify[.]app	Domain
freeanon[.]xyz	Domain
<a href="#">frazza[.]com</a>	Domain
<a href="#">forum[.]ge</a>	Domain
<a href="#">fortuna[.]ge</a>	Domain
<a href="#">footballua[.]tv</a>	Domain
<a href="#">football[.]by</a>	Domain
fly[.]freecluster[.]eu	Domain
<a href="#">fc2f61349e3b9152a43028e0509d10dc[.]safeiframe[.]googlesyndication[.]com</a>	Domain
<a href="#">exk[.]kz</a>	Domain
<a href="#">euroradio[.]fm</a>	Domain
<a href="#">enovosty[.]com</a>	Domain
edufuture[.]biz	Domain
<a href="#">e007c0704f610e92c793531d460e7e90[.]safeiframe[.]googlesyndication[.]com</a>	Domain
<a href="#">dstat[.]sorryy[.]me</a>	Domain
<a href="#">droni[.]ge</a>	Domain
<a href="#">docs[.]google[.]com/document/d/18nxvjQuHPAGRJ-t9S9CJ9dPK9_z0F73UrBpBFn7ZyVo</a>	Domain
<a href="#">digest[.]pia[.]ge</a>	Domain
<a href="#">dev[.]by</a>	Domain
<a href="#">derzhava-sveta[.]webnode[.]ru</a>	Domain

<a href="#">deathputin[.]github[.]io</a>	Domain
ddosrussia[.]netlify[.]app	Domain
ddos[.]featurelab[.]software	Domain
<a href="#">ddos-russian-sites[.]com</a>	Domain
ddos-hohlov[.]vercel[.]app	Domain
<a href="#">d-31801991032363131989[.]ampproject[.]net</a>	Domain
<a href="#">cyber-yuzh[.]com</a>	Domain
<a href="#">cyber-yozh[.]com</a>	Domain
<a href="#">cyber-ukraine[.]com</a>	Domain
<a href="#">c9248b6329f2bcf745f2dc603017afd7[.]safeframe[.]googlesyndication[.]com</a>	Domain
<a href="#">babsi[.]de</a>	Domain
<a href="#">atp[.]gofintechapp[.]com</a>	Domain
<a href="#">asiacharm[.]com</a>	Domain
<a href="#">as104[.]online-stars[.]org</a>	Domain
<a href="#">apteka[.]103[.]by</a>	Domain
<a href="#">antiput[.]in</a>	Domain
<a href="#">amourleague[.]com</a>	Domain
<a href="#">amourfeel[.]com</a>	Domain
<a href="#">amourfactory[.]com</a>	Domain
<a href="#">aif[.]by</a>	Domain
<a href="#">9c6a8bc8c2a9e9e14ce94fc4d280c26[.]safeframe[.]googlesyndication[.]com</a>	Domain
81g6bk[.]csb[.]app	Domain
<a href="#">5sfer[.]com</a>	Domain
<a href="#">24news[.]ge</a>	Domain
<a href="#">ddosohhlov[.]net</a>	Domain
<a href="#">ddos-ukrov[.]netlify[.]app</a>	Domain
<a href="#">help-ukraine-win[.]com</a>	Domain
<a href="#">fuckrff[.]ga</a>	Domain
feraquiziru[.]xyz	Domain
<a href="#">notwar[.]ho[.]ua</a>	Domain
187[.]86[.]129[.]122	IPv4 Address
187[.]86[.]129[.]134	IPv4 Address
187[.]86[.]153[.]254	IPv4 Address

187[.]87[.]189[.]252	IPv4 Address
187[.]87[.]19[.]186	IPv4 Address
187[.]87[.]198[.]250	IPv4 Address
187[.]87[.]200[.]106	IPv4 Address
187[.]92[.]132[.]14	IPv4 Address
187[.]94[.]16[.]59	IPv4 Address
187[.]94[.]209[.]246	IPv4 Address
187[.]94[.]211[.]60	IPv4 Address
187[.]94[.]253[.]81	IPv4 Address
187[.]95[.]112[.]36	IPv4 Address
187[.]95[.]114[.]125	IPv4 Address
187[.]95[.]136[.]10	IPv4 Address
187[.]95[.]136[.]14	IPv4 Address
187[.]95[.]136[.]194	IPv4 Address
187[.]95[.]136[.]46	IPv4 Address
187[.]95[.]136[.]74	IPv4 Address
187[.]95[.]34[.]135	IPv4 Address
187[.]95[.]38[.]17	IPv4 Address
187[.]95[.]80[.]137	IPv4 Address
187[.]95[.]80[.]141	IPv4 Address
187[.]95[.]82[.]45	IPv4 Address
187[.]95[.]82[.]57	IPv4 Address
188[.]0[.]151[.]36	IPv4 Address
188[.]112[.]39[.]231	IPv4 Address
188[.]112[.]39[.]233	IPv4 Address
188[.]116[.]40[.]238	IPv4 Address
188[.]119[.]30[.]75	IPv4 Address
188[.]119[.]30[.]83	IPv4 Address
188[.]120[.]232[.]181	IPv4 Address
188[.]120[.]245[.]247	IPv4 Address
188[.]124[.]12[.]43	IPv4 Address
188[.]124[.]15[.]238	IPv4 Address
188[.]124[.]46[.]55	IPv4 Address
188[.]126[.]45[.]161	IPv4 Address
188[.]126[.]62[.]142	IPv4 Address

188[.]127[.]249[.]9	IPv4 Address
188[.]127[.]250[.]62	IPv4 Address
188[.]130[.]138[.]12	IPv4 Address
188[.]131[.]233[.]175	IPv4 Address
188[.]132[.]241[.]162	IPv4 Address
188[.]133[.]137[.]9	IPv4 Address
188[.]133[.]138[.]197	IPv4 Address
188[.]133[.]139[.]219	IPv4 Address
188[.]133[.]152[.]125	IPv4 Address
188[.]133[.]152[.]247	IPv4 Address
188[.]133[.]152[.]25	IPv4 Address
188[.]133[.]153[.]143	IPv4 Address
188[.]133[.]153[.]161	IPv4 Address
188[.]133[.]153[.]187	IPv4 Address
188[.]133[.]157[.]61	IPv4 Address
188[.]133[.]158[.]145	IPv4 Address
188[.]133[.]158[.]27	IPv4 Address
188[.]133[.]158[.]51	IPv4 Address
188[.]133[.]158[.]80	IPv4 Address
188[.]133[.]160[.]22	IPv4 Address
188[.]133[.]173[.]21	IPv4 Address
188[.]134[.]1[.]49	IPv4 Address
188[.]134[.]88[.]222	IPv4 Address
188[.]134[.]9[.]40	IPv4 Address
188[.]136[.]162[.]204	IPv4 Address
188[.]136[.]162[.]30	IPv4 Address
188[.]136[.]167[.]33	IPv4 Address
188[.]136[.]216[.]201	IPv4 Address
188[.]137[.]82[.]179	IPv4 Address
188[.]138[.]139[.]216	IPv4 Address
188[.]138[.]179[.]13	IPv4 Address
188[.]138[.]205[.]242	IPv4 Address
188[.]138[.]254[.]218	IPv4 Address
188[.]143[.]235[.]128	IPv4 Address
188[.]143[.]235[.]130	IPv4 Address

In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

188[.]143[.]235[.]24	IPv4 Address
188[.]156[.]240[.]240	IPv4 Address
188[.]162[.]227[.]222	IPv4 Address
188[.]163[.]170[.]130	IPv4 Address
188[.]163[.]171[.]198	IPv4 Address
188[.]165[.]119[.]206	IPv4 Address
188[.]165[.]224[.]186	IPv4 Address
188[.]165[.]225[.]139	IPv4 Address
188[.]165[.]226[.]95	IPv4 Address
188[.]165[.]233[.]121	IPv4 Address
188[.]165[.]254[.]122	IPv4 Address
188[.]165[.]45[.]11	IPv4 Address
188[.]165[.]59[.]127	IPv4 Address
188[.]166[.]104[.]152	IPv4 Address
188[.]166[.]115[.]97	IPv4 Address
188[.]166[.]124[.]18	IPv4 Address
188[.]166[.]165[.]240	IPv4 Address
188[.]166[.]252[.]135	IPv4 Address
188[.]166[.]30[.]17	IPv4 Address
188[.]166[.]30[.]24	IPv4 Address
188[.]166[.]34[.]137	IPv4 Address
188[.]166[.]37[.]137	IPv4 Address
188[.]167[.]167[.]3	IPv4 Address
188[.]168[.]22[.]148	IPv4 Address
188[.]168[.]25[.]247	IPv4 Address
188[.]168[.]27[.]71	IPv4 Address
188[.]168[.]28[.]97	IPv4 Address
188[.]168[.]56[.]82	IPv4 Address
188[.]168[.]75[.]254	IPv4 Address
188[.]168[.]81[.]158	IPv4 Address
188[.]169[.]142[.]196	IPv4 Address
188[.]169[.]38[.]111	IPv4 Address
188[.]17[.]158[.]225	IPv4 Address
188[.]170[.]189[.]26	IPv4 Address
8[.]42[.]70[.]4	IPv4 Address

8[.]42[.]71[.]1	IPv4 Address
8[.]42[.]71[.]224	IPv4 Address
8[.]42[.]71[.]225	IPv4 Address
8[.]42[.]71[.]226	IPv4 Address
8[.]42[.]71[.]5	IPv4 Address
8[.]44[.]216[.]242	IPv4 Address
8[.]9[.]36[.]10	IPv4 Address
80[.]106[.]247[.]145	IPv4 Address
80[.]106[.]59[.]35	IPv4 Address
80[.]107[.]16[.]17	IPv4 Address
80[.]109[.]233[.]73	IPv4 Address
80[.]122[.]144[.]182	IPv4 Address
80[.]122[.]183[.]158	IPv4 Address
80[.]123[.]143[.]202	IPv4 Address
80[.]123[.]69[.]54	IPv4 Address
80[.]13[.]0[.]226	IPv4 Address
80[.]13[.]139[.]249	IPv4 Address
80[.]147[.]171[.]88	IPv4 Address
80[.]17[.]254[.]230	IPv4 Address
80[.]191[.]162[.]2	IPv4 Address
80[.]191[.]169[.]66	IPv4 Address
80[.]191[.]169[.]69	IPv4 Address
80[.]191[.]169[.]76	IPv4 Address
80[.]191[.]169[.]79	IPv4 Address
80[.]191[.]169[.]81	IPv4 Address
80[.]191[.]185[.]156	IPv4 Address
80[.]191[.]250[.]162	IPv4 Address
80[.]191[.]40[.]41	IPv4 Address
80[.]191[.]46[.]59	IPv4 Address
80[.]191[.]46[.]60	IPv4 Address
80[.]194[.]87[.]86	IPv4 Address
80[.]210[.]56[.]169	IPv4 Address
80[.]210[.]60[.]178	IPv4 Address
80[.]211[.]23[.]121	IPv4 Address
80[.]233[.]239[.]246	IPv4 Address

80[.]240[.]17[.]59	IPv4 Address
80[.]240[.]202[.]218	IPv4 Address
80[.]240[.]250[.]222	IPv4 Address
80[.]241[.]251[.]54	IPv4 Address
80[.]241[.]44[.]34	IPv4 Address
80[.]243[.]158[.]6	IPv4 Address
80[.]244[.]226[.]92	IPv4 Address
80[.]244[.]228[.]162	IPv4 Address
122[.]200[.]145[.]129	IPv4 Address
122[.]200[.]150[.]133	IPv4 Address
122[.]200[.]150[.]137	IPv4 Address
122[.]200[.]150[.]233	IPv4 Address
122[.]200[.]150[.]249	IPv4 Address
122[.]200[.]93[.]56	IPv4 Address
122[.]224[.]255[.]42	IPv4 Address
122[.]224[.]56[.]198	IPv4 Address
122[.]226[.]176[.]250	IPv4 Address
122[.]226[.]223[.]202	IPv4 Address
122[.]226[.]223[.]221	IPv4 Address
122[.]226[.]224[.]166	IPv4 Address
122[.]226[.]57[.]70	IPv4 Address
122[.]226[.]60[.]69	IPv4 Address
122[.]227[.]236[.]123	IPv4 Address
122[.]228[.]145[.]126	IPv4 Address
122[.]247[.]86[.]4	IPv4 Address
122[.]248[.]197[.]121	IPv4 Address
122[.]248[.]46[.]253	IPv4 Address
122[.]248[.]46[.]26	IPv4 Address
122[.]252[.]179[.]66	IPv4 Address
122[.]254[.]96[.]4	IPv4 Address
122[.]3[.]2[.]56	IPv4 Address
122[.]3[.]205[.]167	IPv4 Address
122[.]3[.]207[.]17	IPv4 Address
122[.]3[.]255[.]114	IPv4 Address
122[.]3[.]41[.]154	IPv4 Address

In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

122[.]4[.]205[.]61	IPv4 Address
122[.]50[.]5[.]98	IPv4 Address
122[.]50[.]6[.]44	IPv4 Address
122[.]50[.]7[.]141	IPv4 Address
122[.]52[.]187[.]137	IPv4 Address
122[.]53[.]82[.]126	IPv4 Address
122[.]54[.]134[.]176	IPv4 Address
122[.]54[.]20[.]50	IPv4 Address
122[.]55[.]185[.]226	IPv4 Address
122[.]55[.]202[.]100	IPv4 Address
122[.]6[.]63[.]36	IPv4 Address
122[.]99[.]125[.]85	IPv4 Address
123[.]1[.]187[.]40	IPv4 Address
123[.]108[.]200[.]106	IPv4 Address
123[.]108[.]201[.]133	IPv4 Address
123[.]108[.]252[.]170	IPv4 Address
123[.]108[.]98[.]108	IPv4 Address
123[.]108[.]98[.]89	IPv4 Address
123[.]120[.]8[.]176	IPv4 Address
123[.]129[.]219[.]11	IPv4 Address
123[.]136[.]29[.]180	IPv4 Address
123[.]138[.]199[.]106	IPv4 Address
123[.]150[.]95[.]142	IPv4 Address
123[.]157[.]100[.]91	IPv4 Address
123[.]157[.]79[.]246	IPv4 Address
123[.]16[.]188[.]2	IPv4 Address
123[.]178[.]142[.]222	IPv4 Address
123[.]18[.]206[.]50	IPv4 Address
123[.]182[.]247[.]247	IPv4 Address
123[.]183[.]174[.]69	IPv4 Address
123[.]200[.]15[.]218	IPv4 Address
123[.]200[.]17[.]107	IPv4 Address
123[.]200[.]19[.]218	IPv4 Address
123[.]200[.]2[.]122	IPv4 Address
123[.]200[.]20[.]6	IPv4 Address

In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

123[.]200[.]22[.]234	IPv4 Address
123[.]200[.]24[.]174	IPv4 Address
123[.]200[.]25[.]130	IPv4 Address
123[.]200[.]31[.]42	IPv4 Address
123[.]200[.]4[.]42	IPv4 Address
123[.]200[.]5[.]210	IPv4 Address
123[.]200[.]6[.]58	IPv4 Address
123[.]200[.]9[.]30	IPv4 Address
123[.]201[.]131[.]62	IPv4 Address
123[.]201[.]21[.]234	IPv4 Address
123[.]203[.]156[.]224	IPv4 Address
123[.]207[.]26[.]92	IPv4 Address
123[.]207[.]94[.]24	IPv4 Address
123[.]213[.]70[.]176	IPv4 Address
123[.]231[.]136[.]59	IPv4 Address
123[.]231[.]141[.]42	IPv4 Address
123[.]231[.]141[.]43	IPv4 Address
123[.]231[.]141[.]45	IPv4 Address
123[.]231[.]141[.]46	IPv4 Address
123[.]231[.]141[.]58	IPv4 Address
123[.]231[.]141[.]61	IPv4 Address
123[.]231[.]141[.]62	IPv4 Address
123[.]231[.]152[.]170	IPv4 Address
123[.]231[.]152[.]171	IPv4 Address
123[.]231[.]152[.]172	IPv4 Address
123[.]231[.]152[.]173	IPv4 Address
123[.]231[.]152[.]174	IPv4 Address
123[.]231[.]185[.]162	IPv4 Address
123[.]231[.]221[.]178	IPv4 Address
123[.]231[.]221[.]242	IPv4 Address
123[.]231[.]221[.]243	IPv4 Address
123[.]231[.]230[.]58	IPv4 Address
123[.]231[.]238[.]221	IPv4 Address
123[.]231[.]242[.]218	IPv4 Address
123[.]234[.]135[.]97	IPv4 Address

123[.]234[.]46[.]51	IPv4 Address
123[.]24[.]187[.]188	IPv4 Address
123[.]253[.]120[.]17	IPv4 Address
123[.]253[.]124[.]28	IPv4 Address
123[.]49[.]48[.]130	IPv4 Address
123[.]49[.]53[.]170	IPv4 Address
103[.]216[.]82[.]22	IPv4 Address
103[.]216[.]82[.]37	IPv4 Address
103[.]217[.]173[.]78	IPv4 Address
103[.]217[.]213[.]125	IPv4 Address
103[.]217[.]213[.]145	IPv4 Address
103[.]217[.]237[.]46	IPv4 Address
103[.]217[.]249[.]1	IPv4 Address
103[.]217[.]249[.]129	IPv4 Address
103[.]217[.]249[.]249	IPv4 Address
103[.]217[.]249[.]250	IPv4 Address
103[.]217[.]249[.]253	IPv4 Address
103[.]217[.]73[.]1	IPv4 Address
103[.]217[.]73[.]125	IPv4 Address
103[.]217[.]73[.]129	IPv4 Address
103[.]217[.]73[.]17	IPv4 Address
103[.]217[.]73[.]33	IPv4 Address
103[.]217[.]73[.]65	IPv4 Address
103[.]217[.]73[.]73	IPv4 Address
103[.]217[.]73[.]9	IPv4 Address
103[.]218[.]102[.]162	IPv4 Address
103[.]218[.]26[.]238	IPv4 Address
103[.]220[.]204[.]101	IPv4 Address
103[.]220[.]206[.]110	IPv4 Address
103[.]220[.]206[.]122	IPv4 Address
103[.]220[.]206[.]53	IPv4 Address
103[.]220[.]207[.]17	IPv4 Address
103[.]220[.]207[.]242	IPv4 Address
103[.]220[.]30[.]61	IPv4 Address
103[.]221[.]253[.]145	IPv4 Address

103[.]221[.]253[.]242	IPv4 Address
103[.]221[.]254[.]102	IPv4 Address
103[.]221[.]254[.]12	IPv4 Address
103[.]221[.]254[.]125	IPv4 Address
103[.]221[.]254[.]7	IPv4 Address
103[.]224[.]145[.]35	IPv4 Address
103[.]224[.]48[.]38	IPv4 Address
103[.]224[.]54[.]225	IPv4 Address
103[.]224[.]54[.]233	IPv4 Address
103[.]225[.]125[.]169	IPv4 Address
103[.]225[.]228[.]21	IPv4 Address
103[.]225[.]89[.]54	IPv4 Address
103[.]226[.]143[.]254	IPv4 Address
103[.]226[.]143[.]86	IPv4 Address
103[.]227[.]145[.]78	IPv4 Address
103[.]227[.]243[.]110	IPv4 Address
103[.]227[.]252[.]66	IPv4 Address
103[.]227[.]252[.]80	IPv4 Address
103[.]227[.]252[.]81	IPv4 Address
103[.]228[.]118[.]78	IPv4 Address
103[.]228[.]246[.]30	IPv4 Address
103[.]228[.]246[.]37	IPv4 Address
103[.]229[.]83[.]106	IPv4 Address
103[.]229[.]85[.]209	IPv4 Address
103[.]229[.]85[.]22	IPv4 Address
103[.]229[.]85[.]234	IPv4 Address
103[.]229[.]85[.]54	IPv4 Address
96[.]30[.]79[.]84	IPv4 Address
96[.]36[.]50[.]99	IPv4 Address
96[.]36[.]8[.]51	IPv4 Address
96[.]38[.]232[.]108	IPv4 Address
96[.]68[.]106[.]185	IPv4 Address
96[.]69[.]76[.]161	IPv4 Address
96[.]72[.]230[.]45	IPv4 Address
96[.]89[.]5[.]21	IPv4 Address

96[.]9[.]66[.]130	IPv4 Address
96[.]9[.]66[.]187	IPv4 Address
96[.]9[.]66[.]200	IPv4 Address
96[.]9[.]66[.]243	IPv4 Address
96[.]9[.]69[.]164	IPv4 Address
96[.]9[.]71[.]18	IPv4 Address
96[.]9[.]71[.]19	IPv4 Address
96[.]9[.]72[.]180	IPv4 Address
96[.]9[.]77[.]71	IPv4 Address
96[.]9[.]77[.]8	IPv4 Address
96[.]9[.]79[.]233	IPv4 Address
96[.]9[.]86[.]70	IPv4 Address
96[.]9[.]87[.]113	IPv4 Address
96[.]9[.]88[.]190	IPv4 Address
96[.]9[.]88[.]194	IPv4 Address
96[.]9[.]88[.]94	IPv4 Address
96[.]9[.]92[.]146	IPv4 Address
96[.]9[.]92[.]200	IPv4 Address
96[.]9[.]92[.]227	IPv4 Address
96[.]91[.]136[.]221	IPv4 Address
96[.]95[.]164[.]41	IPv4 Address
97[.]105[.]14[.]11	IPv4 Address
97[.]74[.]230[.]87	IPv4 Address
97[.]74[.]233[.]206	IPv4 Address
97[.]74[.]6[.]64	IPv4 Address
97[.]87[.]248[.]14	IPv4 Address
98[.]101[.]120[.]1	IPv4 Address
98[.]103[.]88[.]147	IPv4 Address
98[.]115[.]7[.]156	IPv4 Address
98[.]126[.]23[.]24	IPv4 Address
98[.]154[.]21[.]253	IPv4 Address
98[.]162[.]25[.]23	IPv4 Address
98[.]162[.]25[.]29	IPv4 Address
98[.]162[.]25[.]4	IPv4 Address
98[.]162[.]25[.]7	IPv4 Address

## In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

98[.]162[.]96[.]41	IPv4 Address
98[.]162[.]96[.]52	IPv4 Address
98[.]162[.]96[.]53	IPv4 Address
98[.]170[.]57[.]231	IPv4 Address



45305 Catalina cs St 150, Sterling VA 20166