



ThreatMon



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

IT Army of UKRAINE



@threatmon



@MonThreat

Summary	2
Cyber Wars in The Ukraine-Russia War	3
Threat Actor Review: IT Army of Ukraine	4
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
IT Army of Ukraine's Attacks	7
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
IT Army of Ukraine's Attack TTPs	18
IT Army of Ukraine's Attack IOCs	19

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.

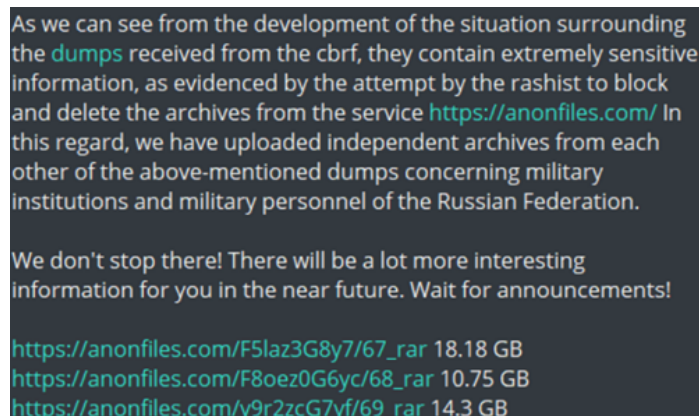
IT Army of Ukraine uses Twitter and Telegram channels to announce the attacks. A website has been created so that more volunteers can participate and the IT Army can install the tools it has developed, and the attacks and the consequences of their attacks are shared on Telegram channels.

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.

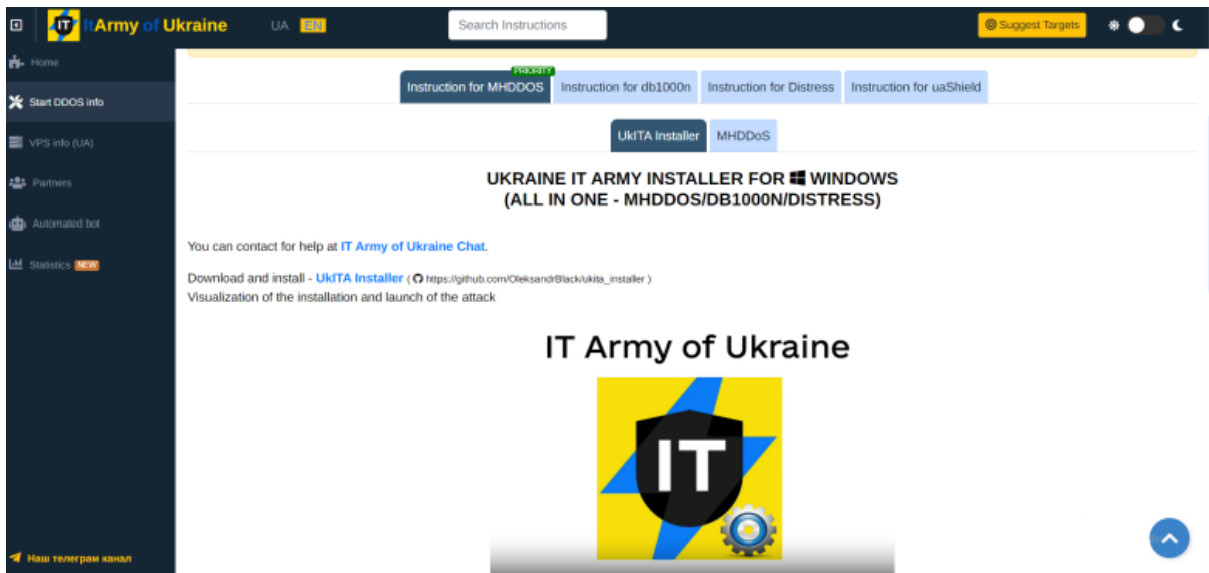
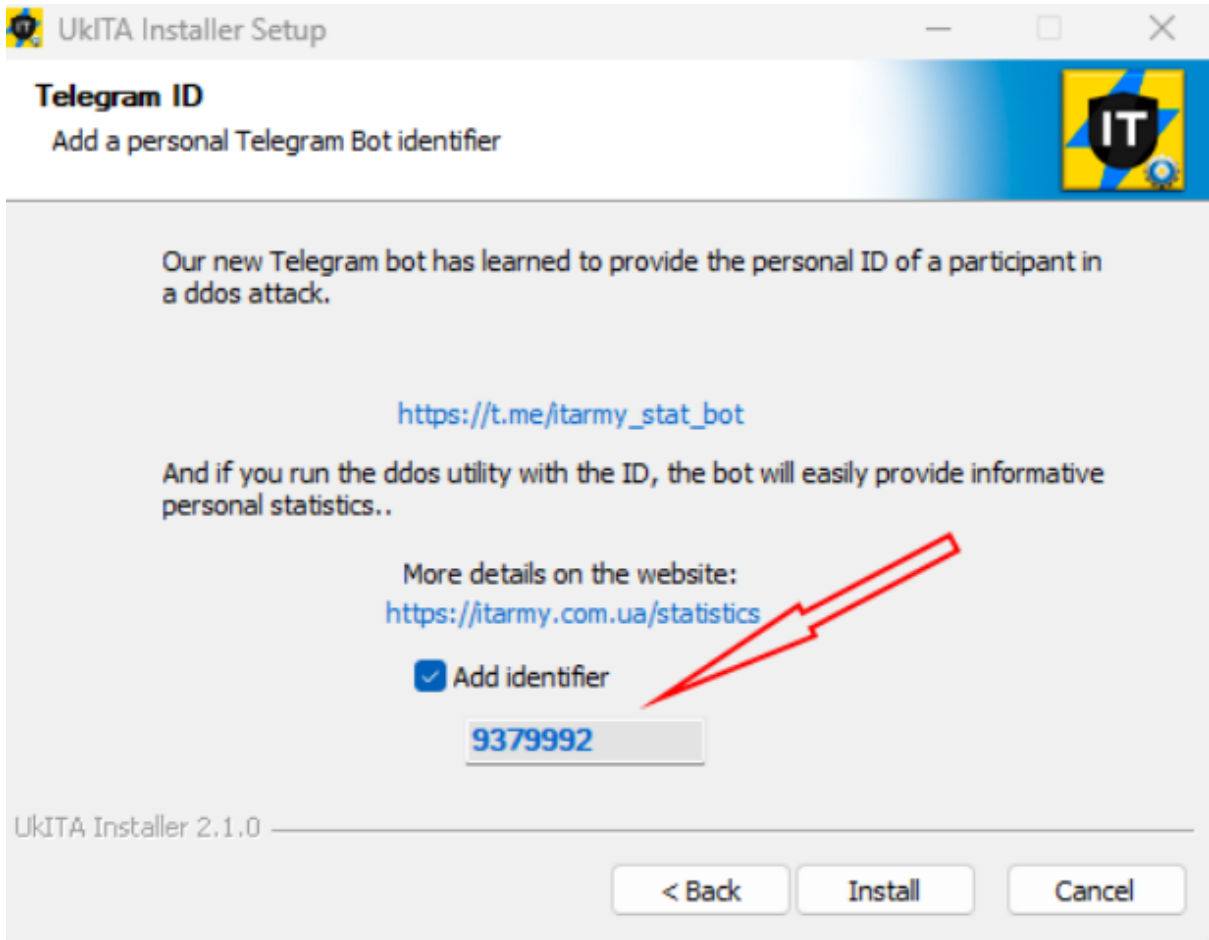


As we can see from the development of the situation surrounding the **dumps** received from the cbrf, they contain extremely sensitive information, as evidenced by the attempt by the rashist to block and delete the archives from the service <https://anonfiles.com/> In this regard, we have uploaded independent 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 18.18 GB
https://anonfiles.com/F8oez0G6yc/68_rar 10.75 GB
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".



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

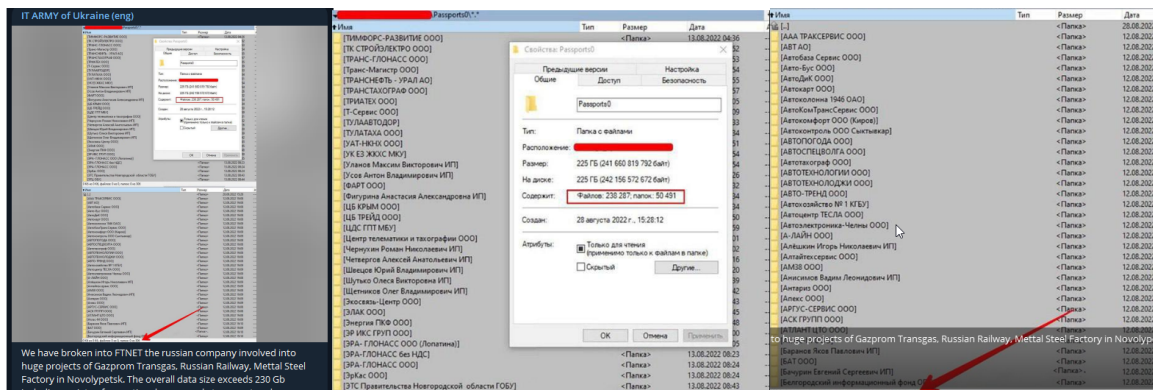
Here are some examples of cyber attacks involving IT Army of Ukraine directly or indirectly:

Example attacks

October 24, 2022

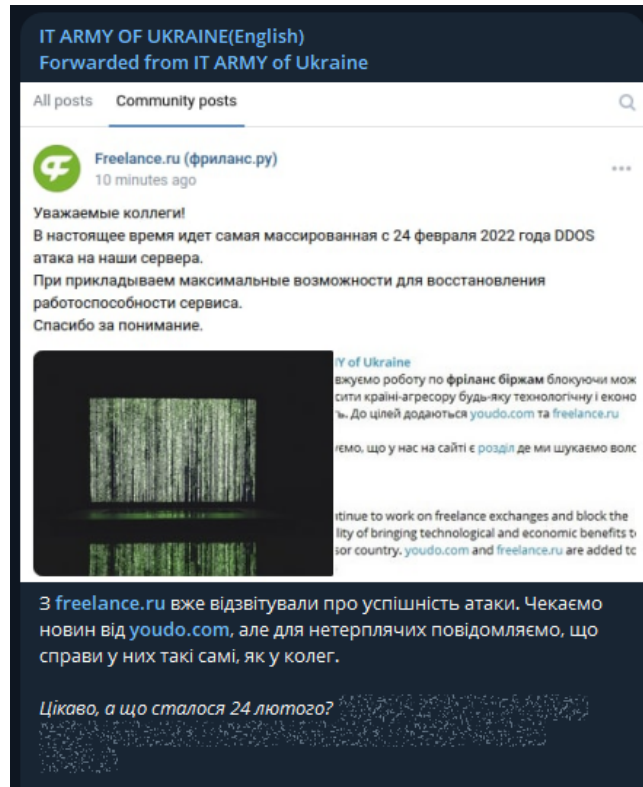
On October 24, 2022, the IT ARMY of Ukraine group accessed and extracted more than 230 Gb of large databases of its victims. This data included various operational documents, transportation and employee profiles.

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

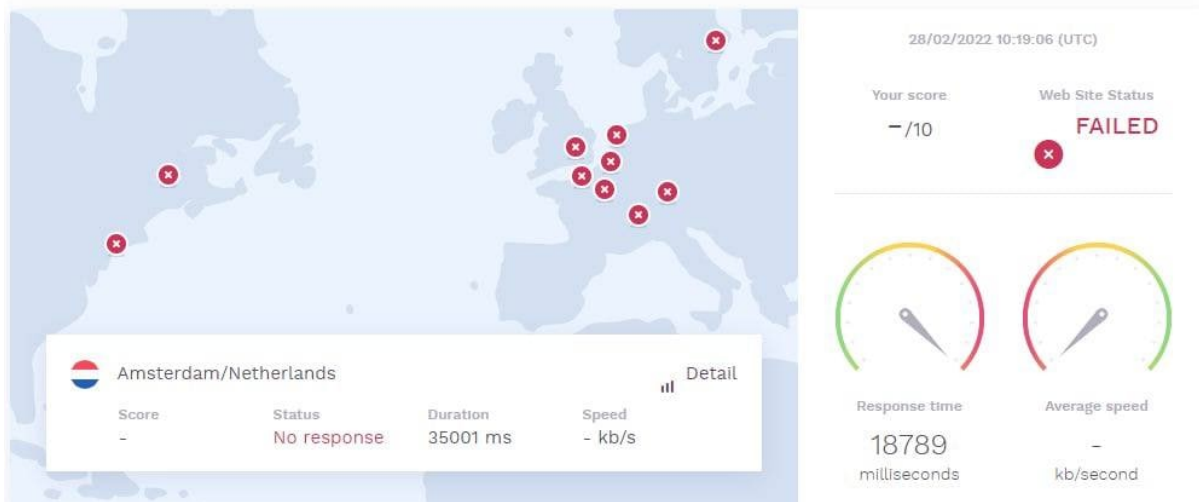
On February 28, 2022, Sberbank main domain and many ATMs became unusable due to DDOS attacks on Sberbank DNS servers.

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

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

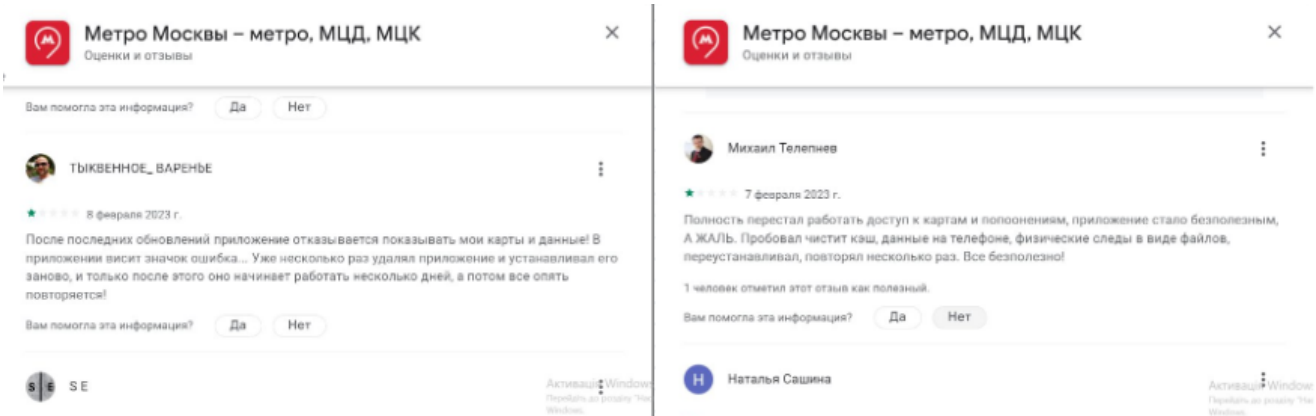
A screenshot of a website article from OFD.RU. The URL is 'ofd.ru/blog/1/ddos-ataki-24-yanvarya-2023-g'. The article title is 'DDoS-атаки 24 января 2023 г.' with a view count of 19. The article content discusses DDoS attacks on fiscal data operators and KKT manufacturers in Russia on January 24, 2023, at 11:50. It mentions that personal cabinets are still accessible but with interruptions, and that data transmission to the FNS is in normal mode. A sidebar on the left contains navigation links: 'Новости', 'Обновления продуктов', 'Цифры и кейсы', 'Видеоролики', 'Инструкции', 'Обзоры продуктов', and 'Вебинары'. The bottom of the article mentions 'онлайн-чатом или чат-ботом'.

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

February 15, 2023

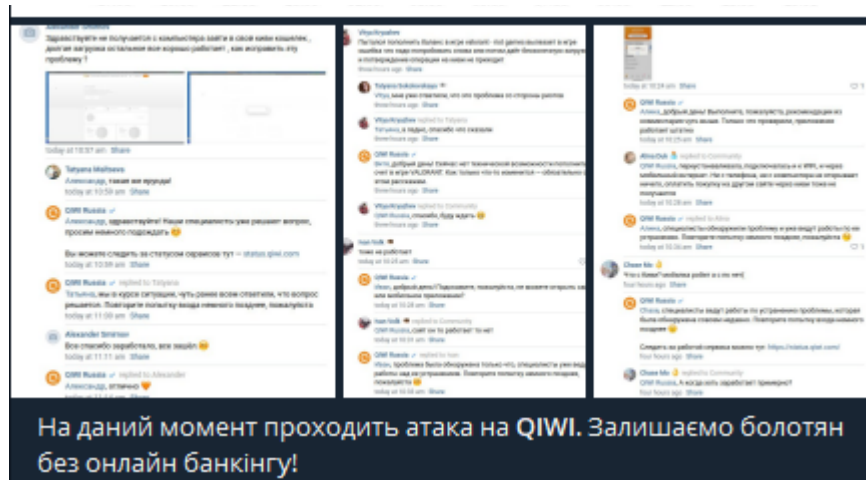
February 15, 2023 They gained access to the corporate network of PayTrans, an IT company that serves the payments of Moscow's normal and medium-capacity metro. It leaked source code for online payment mobile apps, application server for wire transfers, ORA2 and ORA1 for payment transactions, CCTV data.

```
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/
.fbc.sf          vm_bk/
locker/         vm_confluence/
.pb2.sf         vm_delta/
.pbc.sf         vm_first_test/
.sbc.sf         vm_for_test_new_apb/
.sdd.sf         vm_gamma/
.whs.sf         vm_jira/
.iso/           vm_minpromtorg/
vm_ASU_PBK/     vm_mm_suy_kitchen_clone/
vm_AlpineLinux_docker/  vm_nvr/
vm_MM_autodownload_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_autodownload_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-28425aid.vswp': 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.lck': Device or resource busy
rm: can't remove '/vmfs/volumes/datastore0/vm_first_test/vmx-vm_first_test-675437085-1.vswp': 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_minpromtorg/*
rm: can't remove '/vmfs/volumes/datastore0/vm_minpromtorg/vm_minpromtorg-ca46ddb4.vswp': Device or resource busy
rm: can't remove '/vmfs/volumes/datastore0/vm_minpromtorg/vm_minpromtorg-flat.vmdk': Device or resource busy
rm: can't remove '/vmfs/volumes/datastore0/vm_minpromtorg/vm_minpromtorg.vmx.lck': Device or resource busy
```



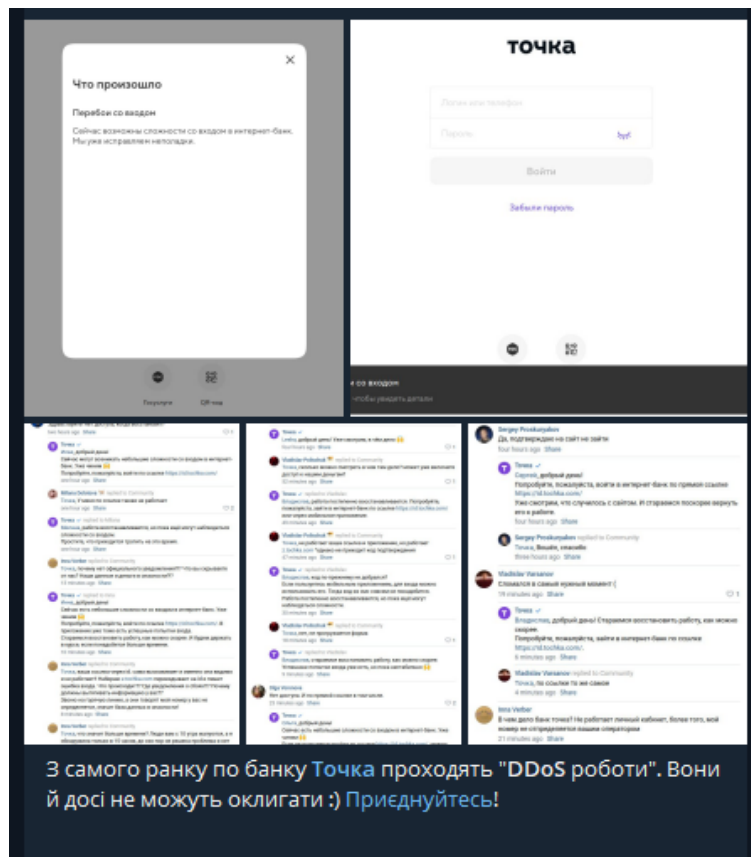
February 20, 2023

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.

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

SecurityLab.ru
by Positive Technologies

Федеральная таможенная служба подверглась DDoS-атаке

41 / 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 словам ФТС, проблема была решена, и работа ресурсов ФТС не прервана. В то же время атаки отразились на работе формоператоров, передающих информацию в таможенные базы.

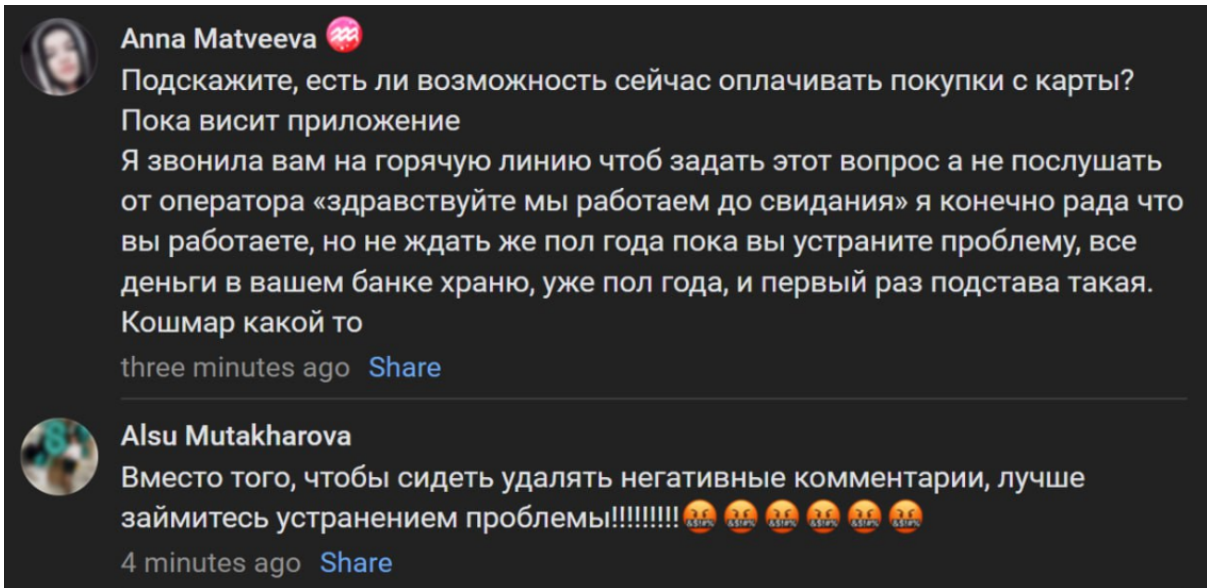
Министерство также отметило, что система электронного декларирования товаров «Альта-Софт» 28 февраля подверглась беспрецедентной кибератаке, которая нарушила процессы таможенного оформления грузов. Систему «Альта-Софт» является одной из самых используемых для подачи данных в таможенную службу.

Вечером 28 февраля «Альта-Софт» разослала клиентам уведомление о массовой DDoS-атаке, которая началась в 8:10 утра и длилась несколько часов. Кибератака привела к сбоям в системе электронного декларирования. В этот же день в 13:00 специалисты компании постепенно восстановили обмен данными с таможенными органами.

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

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.



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 надёжно защищены и останутся в безопасности.

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

Устраняем сбой

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

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

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

Ай Барс Банк
Айс, мы не удаляем негативные комментарии. Удаляем только те...

Ай Барс сообщил о проведении технических работ - Frank
Ай Барс Банк и служба техподдержки уведомили о проведении технических работ: «Следует учесть, что пользователи не смогут получить доступ к...

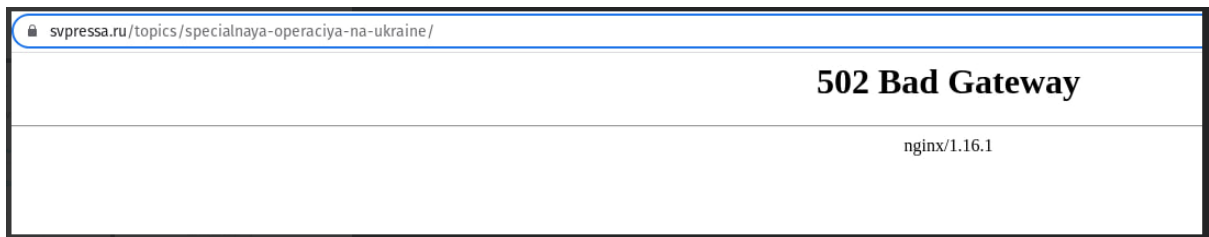
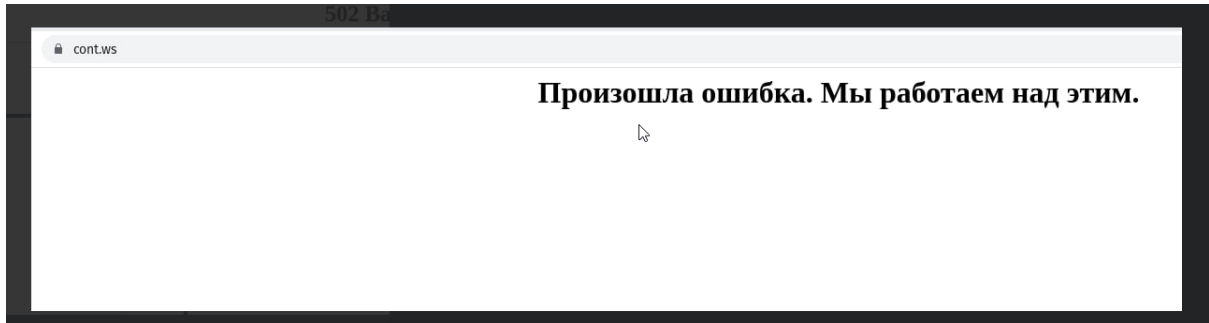
Сервисы «Ай Барс Банка» сбой: в банке обещают наладить работу к 13:00
Сервисы «Ай Барс Банка» сбой: в банке обещают наладить работу к 13:00... Наладить об устранение сбоя: клиенты Ай Барс Банк...

Сервисы Ай Барс Банка сбой: в организации обещают наладить работу к 13:00... Наладить об устранение сбоя: клиенты Ай Барс Банк...

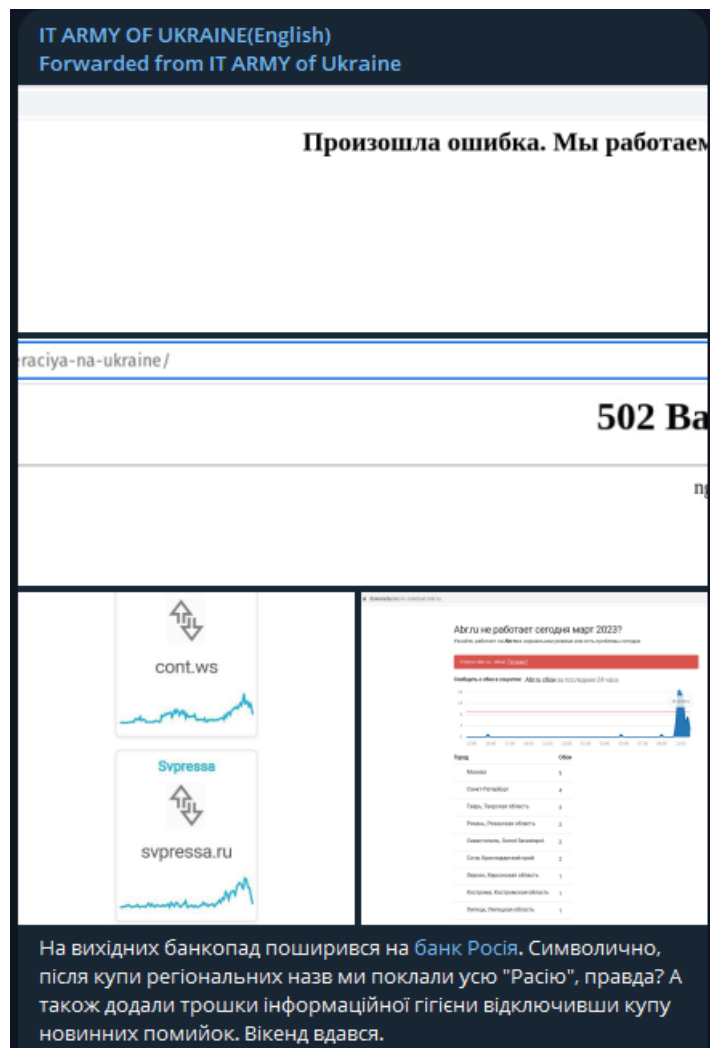
Наступний в черзі недоступних стає банк Барс, який терміново проводить технічні роботи. Нас тільки дивує, що вони всі нічого не роблять поки ми їх не лупанемо як слід. Великий і могутій руський авось, завжди і в усьому. Може їм квіз запусити з питанням: хто наступний?

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

raciya-na-ukraine/

502 Ba

cont.ws

Svpressa

svpressa.ru

ABR.ru не работает сегодня март 2023?
Результаты работы сервера мониторинга за последние 24 часа

Страна	Объем
Россия	1
США	1
Украина	1
Польша	1
Германия	1
Франция	1
Италия	1
Канада	1
Бразилия	1
Индия	1
Южная Африка	1
Австралия	1
Япония	1
Корея	1
Испания	1
Мексика	1
Израиль	1
Индонезия	1
Тайвань	1
Вьетнам	1
Филиппины	1
Малайзия	1
Сингапур	1
Южная Корея	1
Испания	1
Италия	1
Франция	1
Германия	1
Польша	1
Украина	1
США	1
Россия	1

На вихідних банкопад поширився на банк Росія. Символично, після купи регіональних назв ми поклали усю "Росію", правда? А також додали трошки інформаційної гігієни відключивши купу новинних помийок. Вікенд вдався.

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.

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

Не работает Rshb.ru?
Не получается загрузиться, не запускается, не доступен, какой-то глюк?

У меня проблемы с Rshb.ru

ОБЩИЕ ПРОБЛЕМЫ С RSHB.RU

ПРИЛОЖЕНИЕ 100%

Сначала новы ...
Мария Журилова
У меня тоже не работает на приложение на сайт
7 часов тому · Поделился

Dmitry Melnikov
Что с приложением и с сайтом?
15 часов тому · Поделился

Руслан Рудкович
Как скачать приложение то?
вчера о 18:14 · Поделился

Александр Гаврилов
Рублик, не твдд ты собираешься инвестировать
дак тогда току · Поделился

Добрый день! Не получается войти в приложение РСХБ и на сайт. Как долго будут недоступны сервисы? 9:51

ЕЛЕНА ШУРЫГИНА 🤗 БИЗНЕС НА ЛАЙТЕ 📈
Добрый день! Не получается войти в приложение РСХБ... Аналогично) 10:04

FCBS
Увеличились вложения
Нали банк отменяет сотрудничество DDoS атаку атаку...
Нали банк отменяет сотрудничество DDoS атаку атаку...
Нали банк отменяет сотрудничество DDoS атаку атаку...
Мы делаем все возможное, чтобы все сервисы были бы
другими. Спасибо за понимание! Будьте здоровы!

Город	Обои
Москва	10
Челябск, Челябинская	3
Новый Новгород, Новгородская область	2
Копельно, Владимирская область	1
Омск, Омская область	1
Железнодорожный, Челябинская	1
Казань, Татарстан	1
Курганск, Новгородская область	1

о бое в соцсетях: Novikom.ru бои за последние 24 часа

3:00 16:00 19:00 22:00 01:00 04:00 07:00

НЕТ ОТЧЕТОВ

и РСХБ-БРОКЕР

7910-53 ПОНЕДЕЛЬНИК

В нас на каналі було тихо декілька днів, а тим часом палало в ще двох банках - Банк Промисловості та Російський Аграрний Банк. Деякі відновлювальні роботи тривають і досі. Хай тривають, буде чим Україні контрибуцію сплачувати.

Сумнозвісні "Ведомості" попали під програму інформаційної гігієни, тож деякий час їх читачам довелося мучитися без чергової дози пропаганди.

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
www[.]zdg[.]md	Domain
www[.]lusatoday[.]com/search/results?q=	Domain
www[.]ukrinform[.]ru	Domain
www[.]ted[.]com/search?q=	Domain
www[.]stily[.]ge	Domain
www[.]rondevo[.]com	Domain
www[.]psichopatas[.]lt	Domain
www[.]picuki[.]com	Domain
www[.]lostro[.]org	Domain
www[.]onlinedics[.]ru	Domain
www[.]mamywiekszego[.]pl	Domain
www[.]fbi[.]com	Domain
www[.]dynamomania[.]com	Domain
www[.]cia[.]gov/index[.]html	Domain
www[.]bigmir[.]net	Domain
www[.]alial[.]ge	Domain
www[.]abw[.]by	Domain
www[.]11variant[.]ru	Domain
war[.]lt	Domain
vug[.]pl/takeRussiaDown[.]html	Domain
vug[.]pl	Domain
vtemu[.]by	Domain
vlast[.]kz	Domain
v3[.]jrmk[.]net	Domain
ukrainiancharm[.]com	Domain
ukraine[.]is-great[.]org	Domain
ua[.]korrespondent[.]net	Domain
tv8[.]md	Domain
trendy-u[.]com	Domain
the-list[.]ams3[.]cdn[.]digitaloceanspaces[.]com omtarahino[.]notion[.]site/tarahino	Domain

talkytimes[.]com	Domain
talkyminutef[.]com	Domain
talkyhour[.]com	Domain
stoprussianweb[.]eu	Domain
stopputin[.]ddns[.]net	Domain
stop-russian-fake[.]news	Domain
stop-russia[.]synergize[.]co	Domain
stop-russia[.]lrf[.]gd	Domain
stop-russia[.]great-site[.]net	Domain
stop--russian--desinformation-near-page[.]translate[.]goog	Domain
stirif[.]md	Domain
star[.]korupciya[.]com	Domain
slavaukraini[.]online	Domain
slavaukrainif[.]1000webhostapp[.]com	Domain
sbiblio[.]com	Domain
russianwarshipgofuckyourself[.]club	Domain
russia-must-be-stopped-6mpfu[.]ondigitaloc ean[.]app	Domain
ru[.]jjooble[.]org	Domain
romancetale[.]com	Domain
ringside24[.]com	Domain
realist[.]online	Domain
raid[.]shell[.]enes[.]tech	Domain
r[.]search[.]yahoo[.]com	Domain
putler[.]whonnock[.]sk	Domain
putin-huilo[.]xyz	Domain
primetime[.]ge	Domain
pravdatutnews[.]com	Domain
point[.]md	Domain
play[.]tavr[.]media	Domain
pia[.]ge	Domain
peliskovif[.]cz	Domain
peimquizpol[.]xyz/	Domain
padaread[.]com	Domain

padabum[.]com	Domain
ovh1[.]vanagas[.]tech	Domain
osvita[.]name	Domain
omore[.]city	Domain
officiel-online[.]com	Domain
nowar[.]1plus[.]red	Domain
norussian[.]tk	Domain
news[.]bigmir[.]net	Domain
neagent[.]by	Domain
mwlf[.]vdlf[.]pl	Domain
megatv[.]ge	Domain
mbox[.]bigmir[.]net	Domain
mamwykshzego[.]pl	Domain
m[.]valentime[.]com	Domain
m[.]rondevo[.]com	Domain
m[.]orchidromance[.]com	Domain
m[.]loveswans[.]com	Domain
m[.]funchatt[.]com	Domain
m[.]derzhava-sveta[.]webnode[.]ru	Domain
m[.]amourfeel[.]com	Domain
m[.]amourfactory[.]com	Domain
m[.]999[.]imd	Domain
livebeam[.]com	Domain
lady[.]tochka[.]net	Domain
kuzelovi[.]cz	Domain
kratkoef[.]com	Domain
korupciya[.]com	Domain
korrespondent[.]net	Domain
konspiracie[.]tresk[.]sk	Domain
knizhnik[.]org	Domain
kinowar[.]com	Domain
kaszaniok[.]github[.]io	Domain
kanalukraina[.]tv	Domain
joinposter[.]com	Domain
jebacruskich[.]page	Domain

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

deathputin[.]github[.]io	Domain
ddosrussia[.]netlify[.]app	Domain
ddos[.]featurelab[.]software	Domain
ddos-russian-sites[.]com	Domain
ddos-hohlov[.]vercel[.]app	Domain
d-31801991032363131989[.]ampproject[.]net	Domain
cyber-yuzh[.]com	Domain
cyber-yozh[.]com	Domain
cyber-ukraine[.]com	Domain
c9248b6329f2bcf745f2dc603017afd7[.]safeframe[.]googlesyndication[.]com	Domain
babsi[.]de	Domain
atp[.]gofintechapp[.]com	Domain
asiacharm[.]com	Domain
as104[.]online-stars[.]org	Domain
apteka[.]103[.]by	Domain
antiput[.]in	Domain
amourleague[.]com	Domain
amourfeel[.]com	Domain
amourfactory[.]com	Domain
aif[.]by	Domain
9c6a8bc8c2a9e9e14ce94fbc4d280c26[.]safeiframe[.]googlesyndication[.]com	Domain
81g6bk[.]csb[.]app	Domain
5sfer[.]com	Domain
24news[.]ge	Domain
ddoshohlov[.]net	Domain
ddos-ukrov[.]netlify[.]app	Domain
help-ukraine-win[.]com	Domain
fuckrf[.]ga	Domain
feraquiziru[.]xyz	Domain
notwar[.]ho[.]lua	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

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

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

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[.]118	IPv4 Address
96[.]9[.]71[.]119	IPv4 Address
96[.]9[.]72[.]1180	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[.]14	IPv4 Address
98[.]162[.]25[.]7	IPv4 Address

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



ThreatMon



45305 Catalina cs St 150, Sterling VA 20166