

Historical Cyber Warfare – Russia vs Ukraine

February 2022

TABLE OF CONTENTS

Introduction	3
Russia vs Ukraine.....	3
Russia DDoS Attack Against Ukraine	3
HermeticWiper	3
SandWorm Recruitment.....	4
Ukraine Efforts.....	4
Guerilla Warfare.....	4
Phishing Campaigns	6
VPN Joins the Fight	7
Threat Groups Intervene	8
Hacktivists groups Taking Sides	8
Ransomware Groups Taking Sides.....	11
Belarus Is Next?	16
Underground Sanctions Against Russia	19
Business As Usual	19
Summery	20
CONTACT US.....	21

INTRODUCTION

As we witness history in the making, the scale and complexity of the conflict are immeasurable.

When focusing on the cyber warfare aspect of the conflict we can see, first time in history, warfare that includes every type of cyber-personal, state-sponsored groups, ransomware groups, hacktivists, DDoS actors, script kitties and even volunteers that want to join the cause.

This event is one of the most significant in this century given the fact that any civilian in the world can take place in this conflict given a browser and computing power and we see those effects taking place, from websites that break down to multiple data leakage events.

RUSSIA VS UKRAINE

Since the first moment Russia has made the first move, infiltrating into Ukraine, we have witnessed massive attacks against several Ukraine entities. While the first 48 hours comprised of mainly Russian attacks, Ukraine-associated entities and other supporters around the world do their best to compromise and takedown Russian targets as well.

RUSSIA DDOS ATTACK AGAINST UKRAINE

One of the first attacks initiated against Ukraine was a distributed denial-of-servers (DDoS) attack that lead to Ukraine's Defense Ministry, PrivateBank and Oschadbank websites being out of service for several hours. Given the fact that Russia is well funded with resources to initiate such an attack, these targets' odds to stand against this attack are very slim.

HERMETICWIPER

In addition to Russia's efforts to compromise financial and government entities with DDoS attacks, security researchers at ESET, Symantec, and SentinelOne had discovered a costume-made wiper malware, **HermeticWiper**, that is targeting Ukrainian organizations, spreading itself and wiping Windows machines.

Up until now, no group has been linked to HermeticWiper, although given the cases we have seen of Russian campaigns such as WhisperGate in January, and the fact that this wiper utilizes techniques that were used by APT33 and Lazarus group, we can conclude the skill and capabilities that the group that created this wiper has.

The wiper is mainly targeting Ukraine, but it was also witnessed in neighboring countries and allies.

SANDWORM RECRUITMENT

One of the more common speculations around Russia's cyber-warfare against Ukraine is the recruitment of APTs. This is not the first time we see a relationship between certain APTs to the Russian government and Russia's interests.

SandWorm might be the biggest threat group that publicly gets involved in this campaign. SandWorm, aka Unit 74455, is one of Russia's state-sponsored groups that are in charge of major espionage and hacking campaigns against Ukraine for years. the most famous campaign against Ukraine is the NotPetya, while they are also responsible for the Ukraine power grid cyberattack, French presidential election, 2018 Winter Olympics, and targeting several VIP personnel in the US. The group has been active for at least 8 years.

UKRAINE EFFORTS

Although Russia has started this campaign very strongly, causing severe damage to many Ukrainian infrastructures, Ukraine was able to leverage international empathy and their best efforts to cause the same, if not more damage, to Russia in return.

GUERRILLA WARFARE

As the combat technique in the Ukrainian military has turned into somewhat of guerrilla warfare, it seems that In the cyber realm it is not that different. Many Ukrainian entities opened Telegram channels whose purpose is to recruit people from around the world that are willing to fight for Ukraine and take part in its' cyber warfare efforts.

The nature of these groups is encouraging their members to perform DDoS attacks on Russian targets by command while the admins offer guidance and tools to do so (Figure 1).

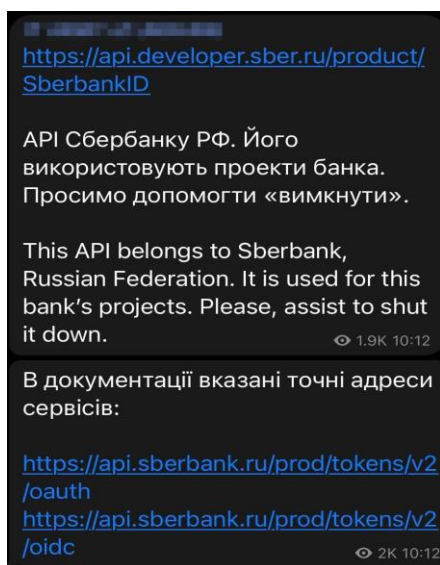


Figure 1: DDoS attacks instructions published on Russian targets

Furthermore, several websites were created in order to initiate and monitor DDoS attacks that are being deployed against Russian institutes at any given moment (Figure 2).

URL	Number of Requests	Number of Errors
https://[REDACTED]	2674	16
https://[REDACTED]	1678	16
https://[REDACTED]a/	1680	16
https://[REDACTED]ru/	1684	16
https://[REDACTED]om/	1678	17
http://[REDACTED]/	1696	1696
http://[REDACTED].ru/	1696	1696
https://[REDACTED]u/	1680	17
https://[REDACTED]	1699	17
https://[REDACTED]ru/	1680	17
https://[REDACTED].ru/	1690	17
https://[REDACTED]ru/	1684	17
https://[REDACTED]i.ru/	1674	17
https://[REDACTED]erbank.ru/	1676	17
https://[REDACTED]ru/	2126	17
https://[REDACTED]ov.ru/	2780	34
https://[REDACTED]uslugi.ru/	2121	17
https://[REDACTED]	1676	17
https://[REDACTED]ru/	1679	17
https://[REDACTED]	1677	17
https://[REDACTED]	1675	17
https://[REDACTED]rfax.ru/	1677	17
https://[REDACTED].ru/uslugi/	1675	17
http://[REDACTED]nt.ru/	1695	1695
https://[REDACTED]	1674	17
https://[REDACTED]g.gov.ru/	1675	17
https://[REDACTED]gov.ru/	1674	17
https://[REDACTED]/	1678	17
https://[REDACTED]u/	1674	17
https://[REDACTED]prombank.ru/	1682	17
https://[REDACTED]ru/	1675	17
https://[REDACTED]prom.ru/	1678	17
https://[REDACTED]	1674	17
https://[REDACTED]/	1674	17
https://[REDACTED]nickel.com/	1676	17
https://[REDACTED]utneftegas.ru/	1681	17
https://[REDACTED]eft.ru/	1673	17
https://[REDACTED]z.com.ru/	1679	17
https://[REDACTED]/	1678	17
https://[REDACTED]r.ru/	1675	17
https://[REDACTED]erstal.com/	1674	17
https://[REDACTED]alloinvest.com/	1688	17
https://[REDACTED]/	1677	17
https://[REDACTED]p.ru/ru/	1674	28
https://[REDACTED]-group.ru/	1674	17
https://[REDACTED]	1678	17
https://[REDACTED]om/ru/	1688	17
https://[REDACTED]kali.com/en/	1685	17
https://[REDACTED]sib.ru/	1677	17
https://[REDACTED]	1683	17
https://[REDACTED]	1681	17
https://[REDACTED]ws.com/	1680	17
https://[REDACTED]news.ru/	1686	17
https://[REDACTED]lt/	2149	17
https://[REDACTED]ws.ru/	1686	17
https://[REDACTED]u/	1690	17
https://[REDACTED]	1673	17
https://[REDACTED]om/	1675	17
https://[REDACTED]ltic.ru/	1678	16
https://[REDACTED].ru/	3866	48

Figure 2: Ukrainian website that monitors DDoS attacks on Russian websites.

Cyber-Ukraine

Choose websites for DDoS-Attack

[DDoS russian news](#)
[DDoS russian polity](#)
[DDoS rbc.ru](#)

Russian banks DDoS temporarily not available

Figure 3: Ukrainian website that designed to initiate DDoS attack

PHISHING CAMPAIGNS

It seems that Ukrainian supporters puts more efforts into campaigns targeting Russian assets and pro-Russia groups even when it comes to Telegram and other communication channels. Several Phishing campaigns were witnessed in Russian Telegram groups (Figure 4) in order to compromise Russian civilians.

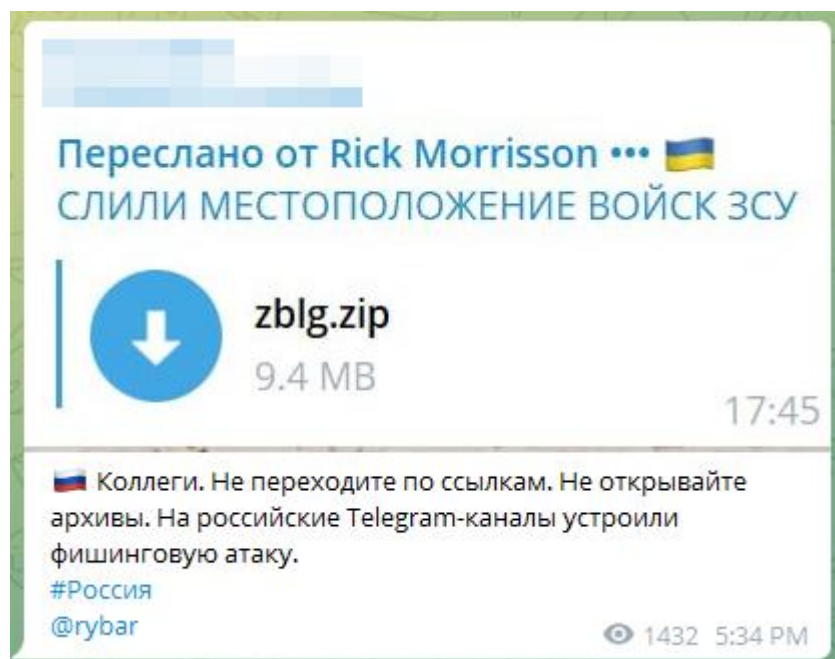


Figure 4: Russian Telegram group admin warns from Ukrainian Phishing campaigns

VPN JOINS THE FIGHT

The Ukrainian supporters leading this whole campaign against Russia also provides tools and techniques to keep the anonymity of everyone who choose to join the fight.

With a corporation with ClearVPN, they have been able to provide a free VPN license to everyone that will join the cause (Figure 5).

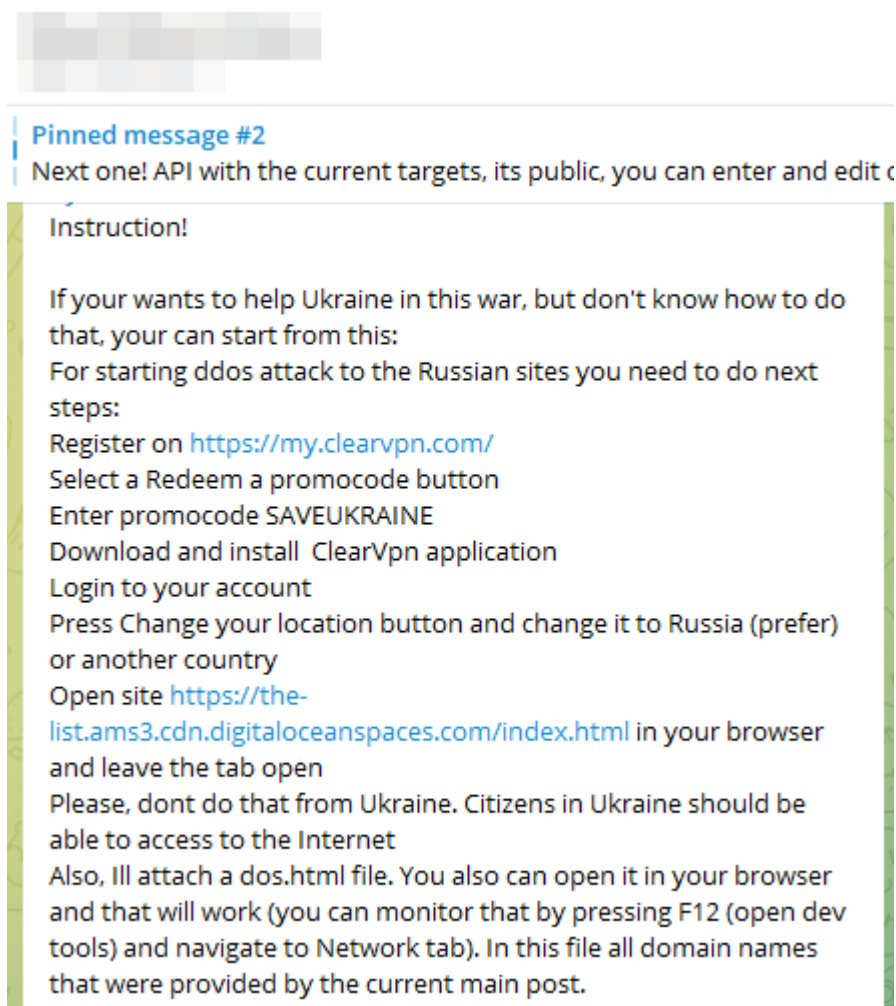


Figure 5: Ukrainian Telegram group offers free ClearVPN promo code: SAVEUKRAINE.

THREAT GROUPS INTERVENE

Given the fact that a hefty number of threat groups, of all kinds, are based around Russian and Ukrainian districts, it is obvious that some will take part in the conflict.

While some remained “apolitical”, the groups that are more emotionally involved or have solid relations with the Ukrainian or Russian government took sides and turn against each other.

HACKTIVISTS GROUPS TAKING SIDES

ANONYMOUS

One of the first groups to take sides was Anonymous which is unsurprising given the fact that they are notoriously known for thriving under political conflicts. The group has announced they will fully support Ukraine and do whatever is within their power to harm Russia’s infrastructures and already published leaked sensitive information about government personnel.

NB65

Not far after Anonymous joined the fight against Ukraine, NB65 have published an announcement claiming they are supporting Ukraine and declared a successful campaign against the Nuclear Safety Institute, and published sensitive documents.



Figure 6: NB65 Twitter post announcing on the Moscow’s Nuclear Safety Institute leak

BELARUSIAN CYBER PARTISANS

Notoriously known for the Belarusian Railway Ransomware campaign several weeks back, the Belarusian Cyber Partisans still has a foothold or backdoor into the Belarusian Railway infrastructure and they are forcing a manual operation of the railways which significantly slows the delivery of Russian troops and supplies to the Russian forces in Ukraine, they keep giving live updates of their actions in their official Telegram channel (Figure 7).

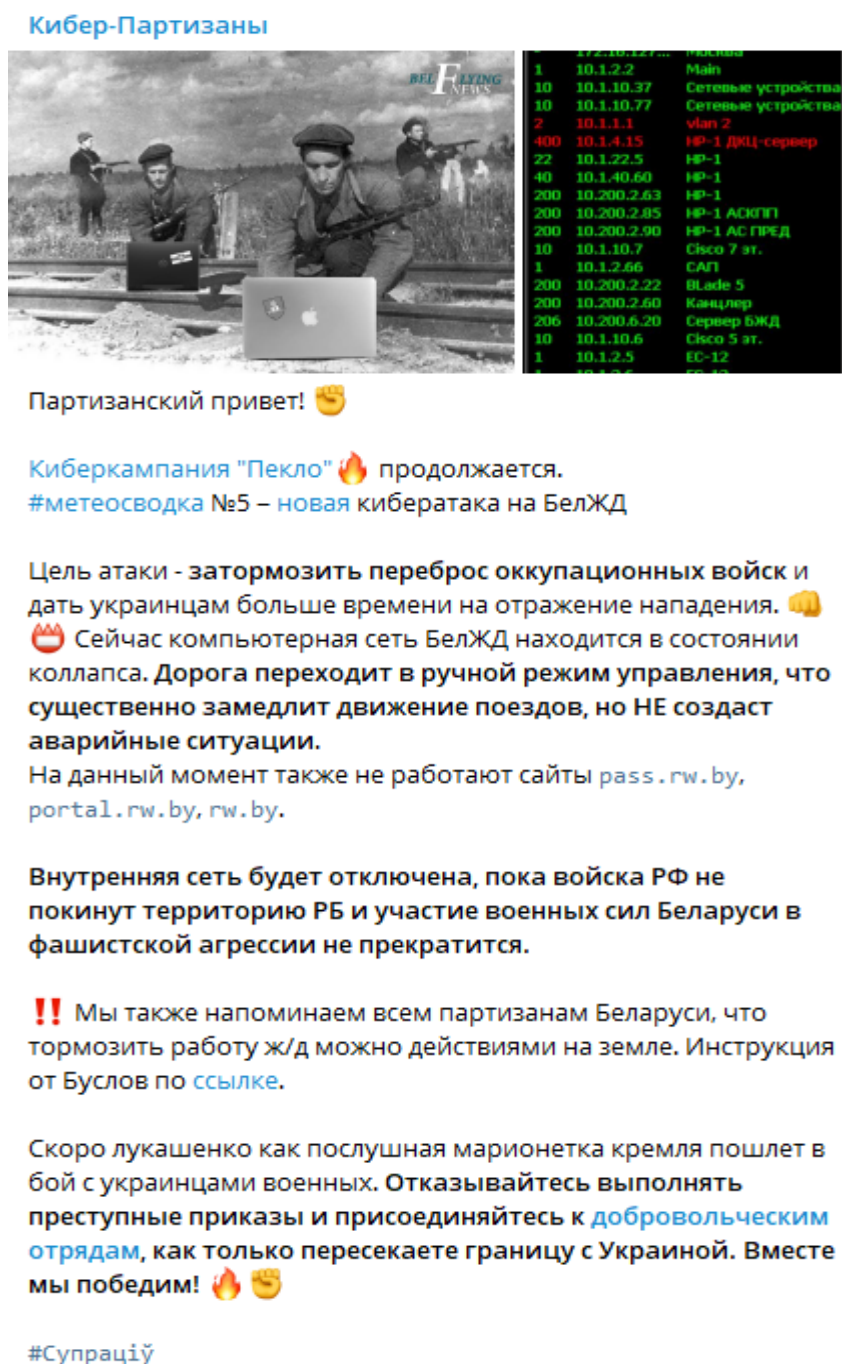


Figure 7: Belarussian Telegram channel announcing the Belarussian Railway compromise

GHOSTSEC

GhostSec is a fairly new hacking group that we have seen going more active since the start of the operation. While siding with the Ukraine, they have put their best efforts into hacking and taking down tactical Russian targets such as banks servers, TV Channels and more.

BLACKHAWK

BlackHawk is a Georgian DDoS group that have initiated DDoS attacks against Russian targets. they have opened a dedicated site to monitor all their DDoS attack in a given moment (Figure 8).

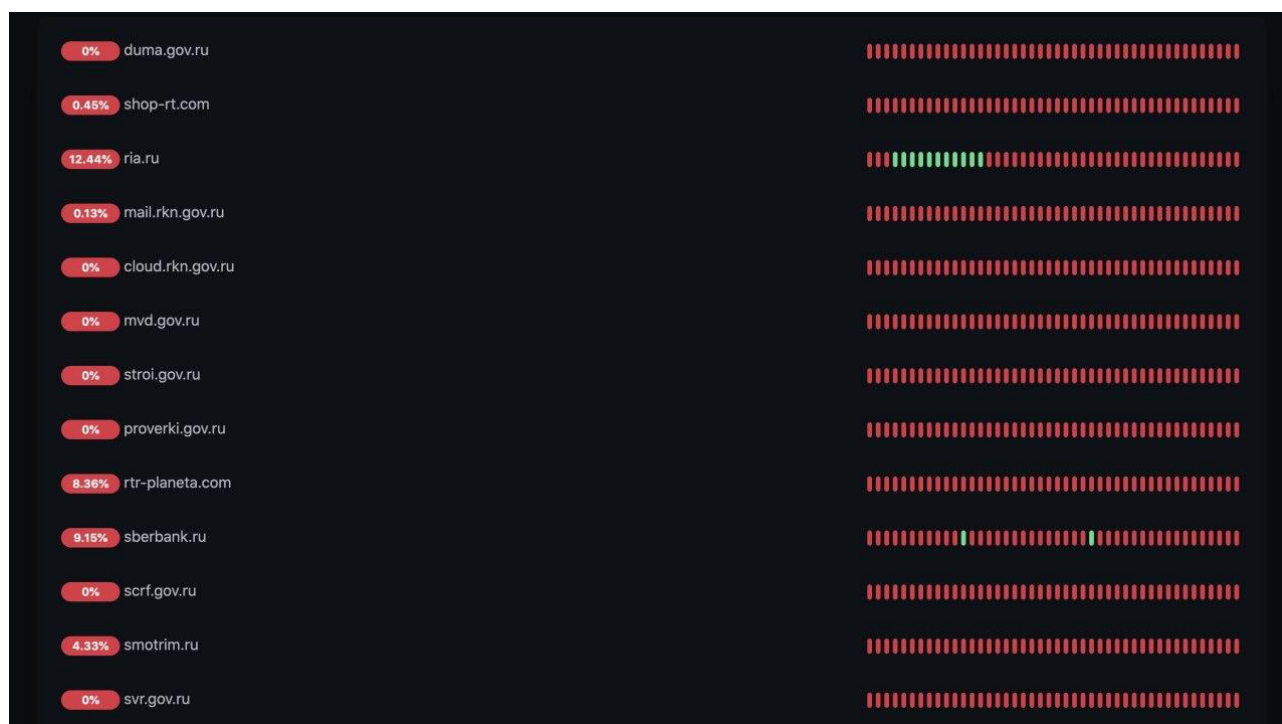


Figure 8: All Russian websites that were attacked by BlackHawk

THE RED BANDITS

The war between Russia and Ukraine has drawn many groups such as GhostSec and BlackHawk from the shadows to brag about their exploits in social media and The Red Bandits is no different.

The Red Bandits, a pro-Russia hacking group, that opened its Twitter account at the beginning of this war and leaked all the sensitive information they can obtain against Ukraine (Figure 9). The group itself appears to be active since early 2021.



Figure 9: The Rad Bandits Twitter post regarding the leaked Ukrainian information

RANSOMWARE GROUPS TAKING SIDES

AGAINSTTHEWEST

AgainstTheWest a double-extortion ransomware group, which is in charge of data leak campaigns in the US and China, also sided with Ukraine and already made some significant custom-made ransomware campaigns against Russia and published all the relevant information in their internal Telegram group (Figure 10).

AgainstTheWest

We've just breached:

- Russian Space Forces
- Ministry of Transport of Russia
- AIP of the Russian Federation
- Russia Air

=====

=====

We've placed a custom-made
ransomware, no RaaS or anything.
Network is unusable for the Russians.

Figure 10: AgainstTheWest announcement of several breaches in Russian defense and government targets

COOMINGPROJECT

While many threat groups are looking to make their appearance and show the world, they are active on the battlefield, some groups might regret coming out to the spotlight. One of them is CoomingProject, a French threat group that announced that they would retaliate if Russia becomes the target of cyberattacks (Figure 11).

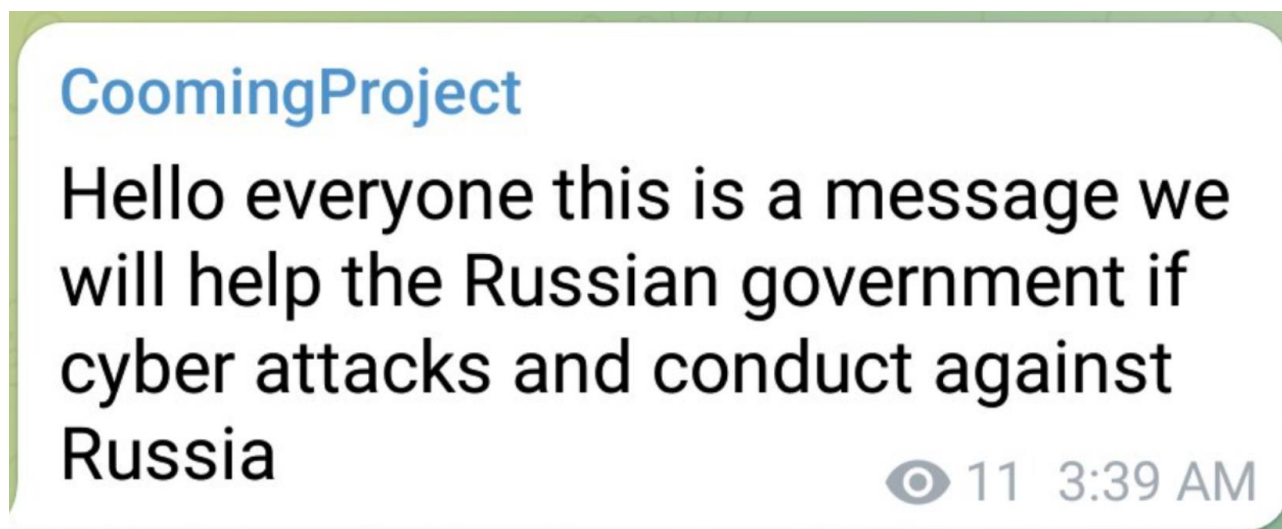


Figure 11: CoomingProject announcement taking sides with Russia

Unfortunately for the ransomware gang, assembled in 2020, this announcement caught the attention of AgainstTheWest, a group that support Ukraine, attention, and the later was able to compromise and leak the identification of CoomingProject members, allegedly six young adults that are based in France. They have made the announcement on both their Telegram channel and their Twitter account (Figure 12,13).



Figure 12: AgainstTheWest triumph against CoominProject

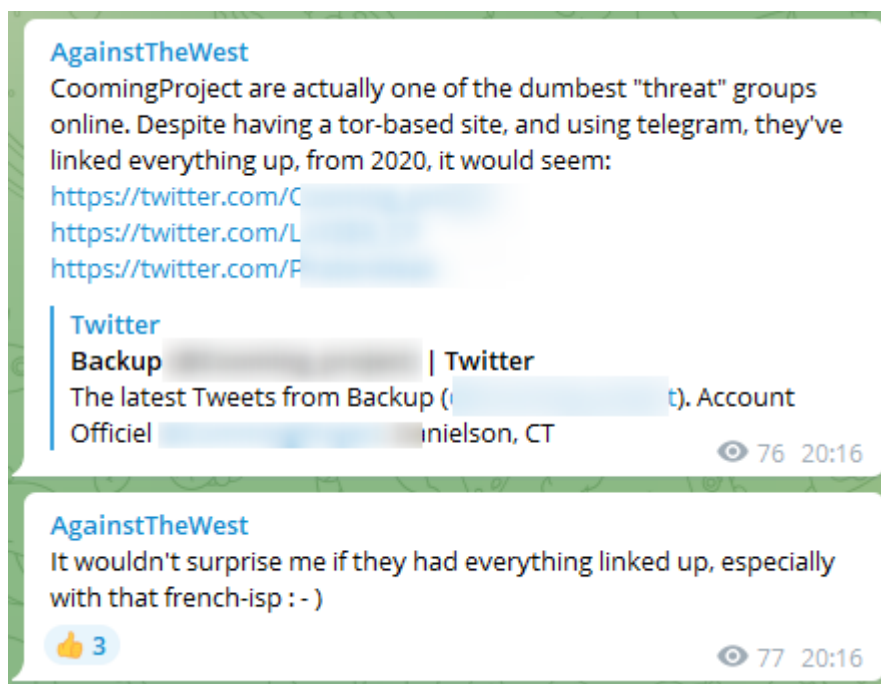


Figure 13: AgainstTheWest Telegram channel publishing their data on CoomingProject

CONTI GROUP REVEALS IT'S TRUE FACE

Conti group is one of the most talented ransomware groups at the moment and they had the highest number of successful campaigns in 2021. Ever since the beginning of this campaign, we have monitored the reaction of Conti and Lockbit2.0 to the matter, trying to see and understand which side they are going to take.

The story of Conti is complex when it comes to this conflict. The first announcement included a firm stance against Ukraine while Conti said that they fully support Russia (Figure 14).

“WARNING”

💬 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

📅 2/25/2022

👁 39

📄 0 [0.00 B]

Figure 14: Conti's first announcement

While their Tor site looks confident, it seems that inside the group the announcement hit massive waves given an emotional effect on the Ukrainian members of the group and sooner than later they have published a rephrase of their announcement declaring that they will support the Russian Federation only against the West and will not side with any government (Figure 15).

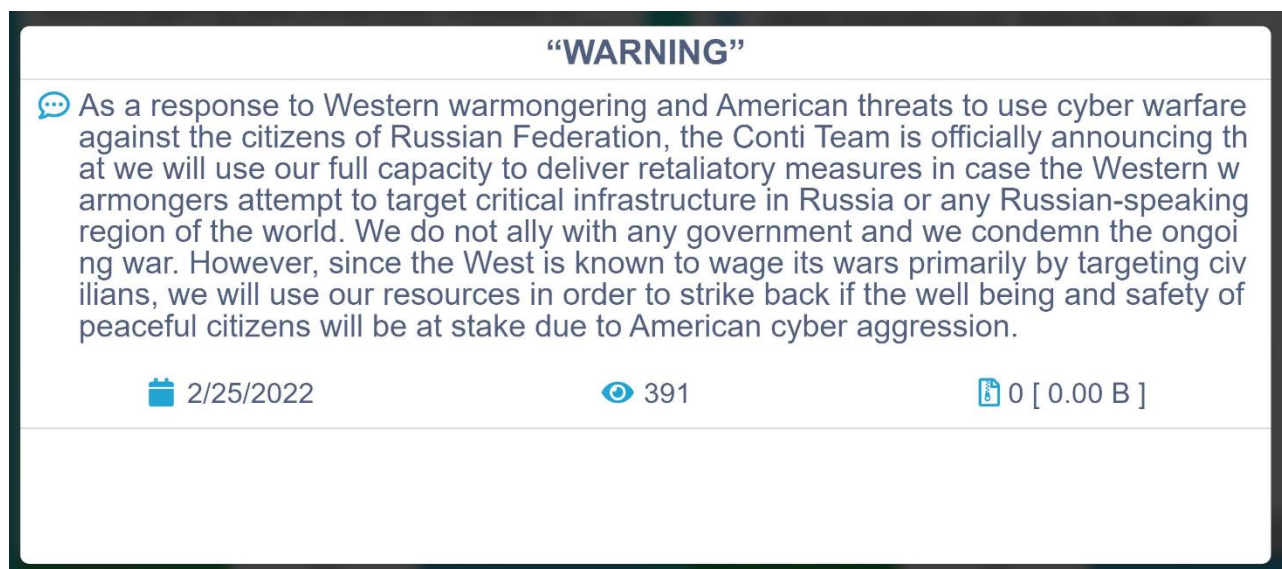


Figure 15: Conti’s rephrased announcement

Several hours after the announcement Ukrainian researcher leaked highly sensitive data of the group including their training plans for newcomers, full Jabber conversation history from the last 13 months including affiliates and operators, Toolkit source code with a promise that more content is on the way (Figure 16).

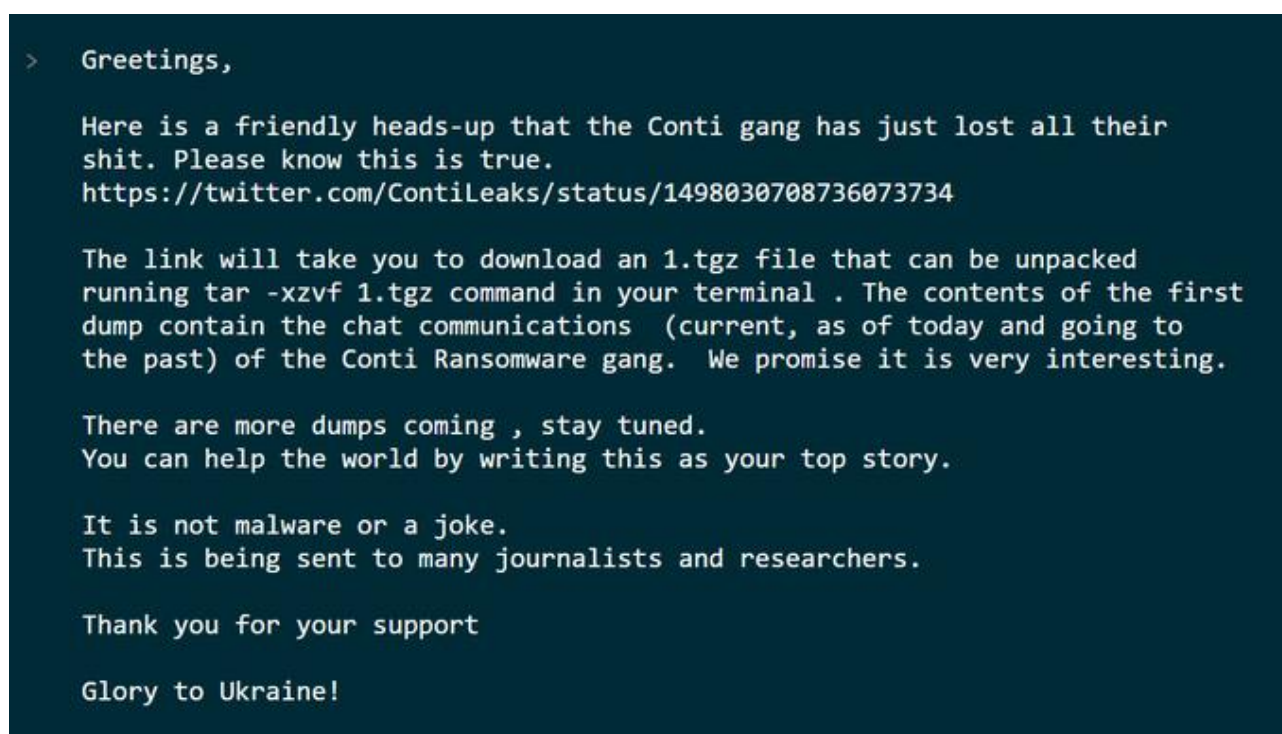


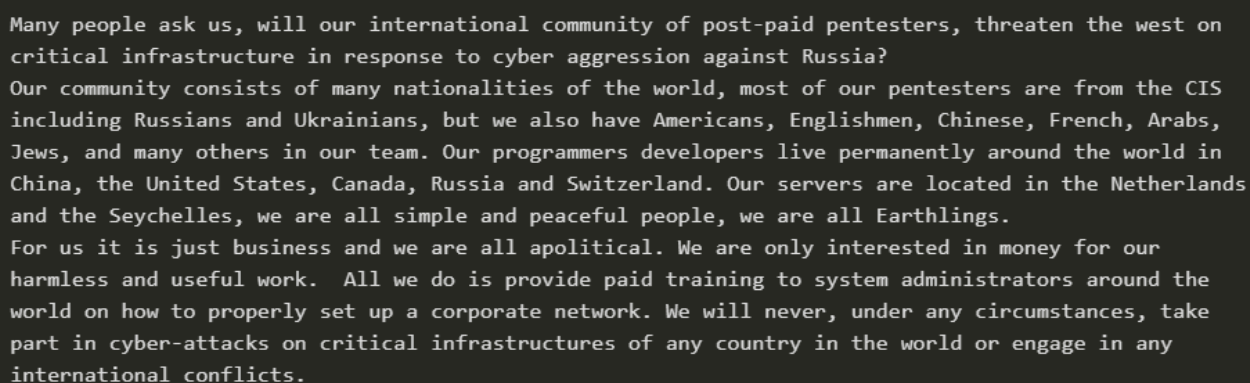
Figure 16: The Ukrainian Researcher First Leak

The massive leak in particular and the way Conti decided to handle this conflict, in general, have caused severe damage to the group and give us some understanding regarding the group’s members’ maturity

and professionalism. In cases in which the default languages of the victim's machine are from Kazakhstan, Uzbekistan, Azerbaijan, Belarus, and Russia, the stealer will not proceed with its actions.

LOCKBIT2.0 - "IT'S ALL ABOUT GOOD BUSINESS"

In contrary to most threat groups, including Conti, Lockbit2.0 have handled the situation differently and did not wanted to make any irrational decisions. With great anticipation from the cyber security community, Lockbit2.0 have made their announcement yesterday with one simple message - This is an apolitical business and no sides will be taken (Figure 17).

A screenshot of a text message with a black background and white text. The text is a statement from Lockbit2.0, explaining their community's composition and their stance on politics and cyberattacks. The text is as follows:

Many people ask us, will our international community of post-paid pentesters, threaten the west on critical infrastructure in response to cyber aggression against Russia?
Our community consists of many nationalities of the world, most of our pentesters are from the CIS including Russians and Ukrainians, but we also have Americans, Englishmen, Chinese, French, Arabs, Jews, and many others in our team. Our programmers developers live permanently around the world in China, the United States, Canada, Russia and Switzerland. Our servers are located in the Netherlands and the Seychelles, we are all simple and peaceful people, we are all Earthlings.
For us it is just business and we are all apolitical. We are only interested in money for our harmless and useful work. All we do is provide paid training to system administrators around the world on how to properly set up a corporate network. We will never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world or engage in any international conflicts.

Figure 17: Lockbit2.0 announcement

It seems that Lockbit2.0 is looking to make the best out of Conti's and other ransomware group situations that are taking part in the conflict and looking to add more victims to their leak site with four new victims since the announcement and eight overall since the weekend.

Furthermore, some speculation suggests that Lockbit2.0 is looking to buy the Emotet/Trickbot botnet - one of Conti's main delivery methods. This strategic buy might cause additional damage to Conti's recovery.

BELARUS IS NEXT?

As part of the Cyberint Research Team's efforts to monitor the full picture of this conflict, several threat groups, both professional and amateur claim that Belarus is the next target. Evidence suggests that DDoS attacks already began against Belarus government infrastructures.

As mentioned, the threat group Belarusian Cyber Partisans, known to us from the first political ransomware in the Belarusian Railway campaign, still has a foothold and blocks or slowing down the transportation of troops and supplies to Russian forces.

Hacktivist group named "IT ARMY of Ukraine" calls out to target Belarusian media in order to end censorship in Belarus (Figure 18).

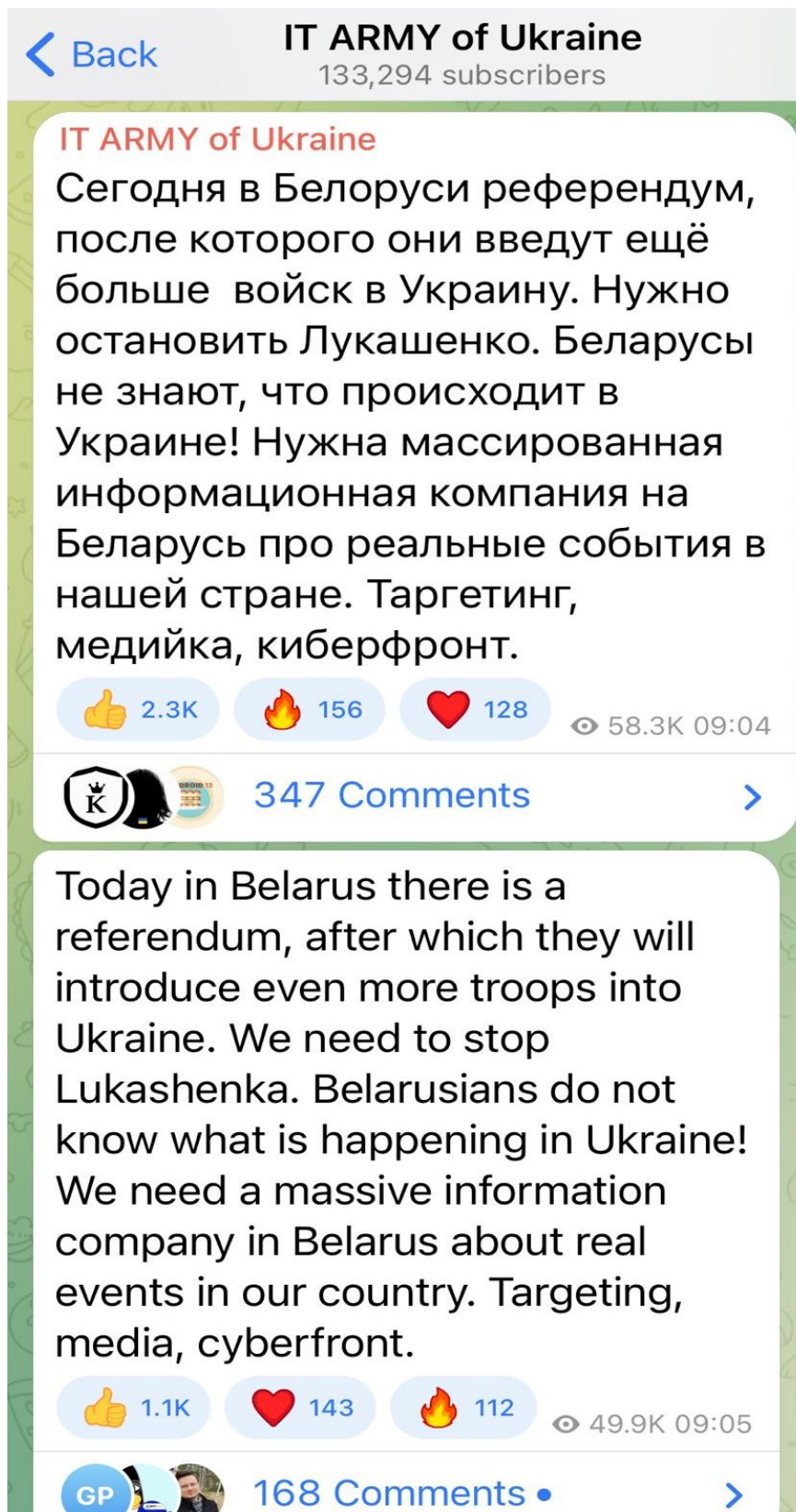


Figure 18: IT ARMY of Ukraine Telegram channel calling to target Belarus media

In addition, many DDoS attacks have already taken place by the same group and hacking volunteers from around the world and some Belarusian websites are already down (Figure 19).

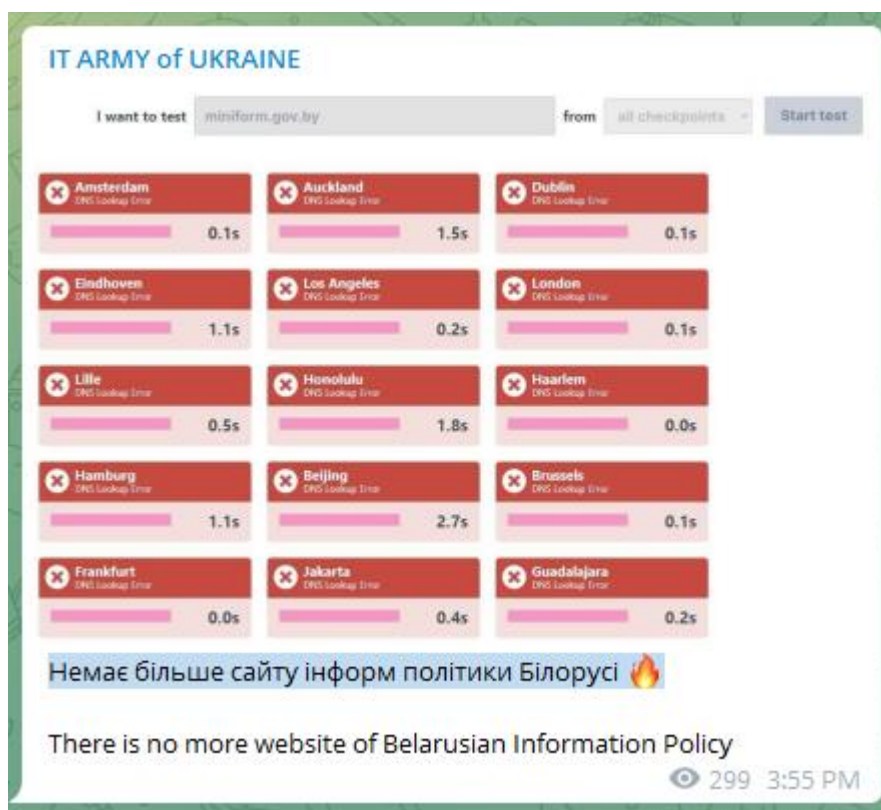


Figure 19: IT ARMY of Ukraine shows Belarusian website that that they attacked successfully

UNDERGROUND SANCTIONS AGAINST RUSSIA

Right before the popular underground forum “Raidforums” was taken down in a security incident, a public announcement from one of the admins shows strict policy against users that are logging in to the forum from Russia, with the claim that these users will be banned from the forum (Figure 20).

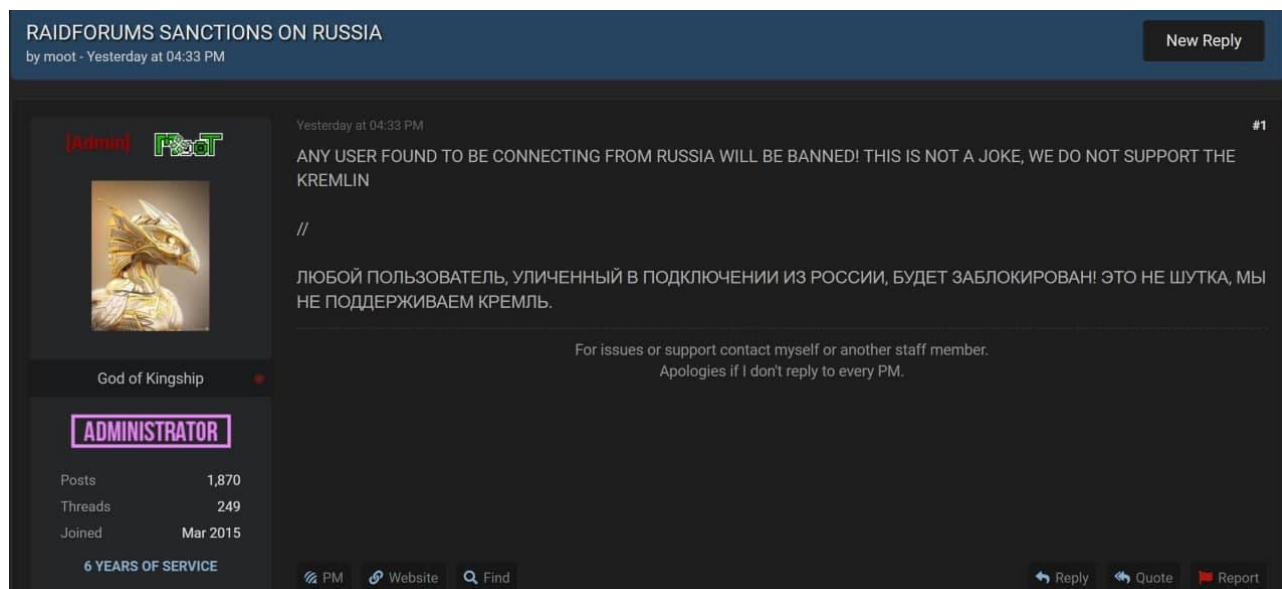


Figure 20: RaidForumes Admin announcing that Russian users will be banned

BUSINESS AS USUAL

While many groups have sided with Russia or Ukraine, it seems that the rest of the groups that kept a safe distance from this conflict are thriving and doing business as usual. As mentioned, Lockbit2.0 puts their efforts to expand their operation and take advantage of the situation.

Another example of a group that had a successful campaign since the beginning of the conflict is the ransomware group LAPSU\$ has compromised and leaked NVIDIA sensitive files.

The interesting part of this campaign was the group’s claim that after the compromise, NVIDIA initiated an attack against the group’s servers and deployed ransomware (Figure 21).

EVERYONE!!! NVIDIA ARE CRIMINALS!!!!!!!!!!

SOME DAYS AGO A ATTACK AGAINST NVIDIA AND
STOLE 1TB OF CONFIDENTIAL DATA!!!!!!

TODAY WOKE UP AND FOUND NVIDIA SCUM HAD
ATTACKED ****THE**** MACHINE WITH
RANSOMWARE.....

LUCKILY IT HAD A BACKUP BUT WHY THE FUCK
THEY THINK THEY CAN CONNECT TO **THE** PRIVATE
MACHINE AND INSTALL RANSOMWARE!!!!!!!!!!!!

Figure 21: Ironic complains by LAPSU\$ to NVIDIA

Given the scale and reputation of NVIDIA, it is highly unlikely this is true.

SUMMARY

The conflict gave the so-called “legitimacy” for the threat groups and many hacktivists to step out from the shadows and go openly on social media about their contribution to rather Russia or Ukraine.

At the moment it seems that as long as this campaign is taking place, we will be able to see more cases of opponent groups going against each other and civilians from around the globe helping the cause of hacktivist groups while it is also likely that we will see threat groups also targeting specific personal within the Belarus, Ukraine and Russia (including Russian oligarchs), in order to assert even more pressure on the shot callers of this conflict.

Given that this complex conflict gives us the opportunity, as researchers, to understand better the minds and techniques of infamous threat actors and threat groups, rather if it's by skill, relations to governments and more, we can only assume that the consequences of this conflict might change the balance of forces and relationships in the threat landscape as we currently know it worldwide.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City