Russia or Ukraine: Hacking groups take sides

therecord.media/russia-or-ukraine-hacking-groups-take-sides/

February 25, 2022

Image: Luis Villasmil

Updated March 3 at 7:35pm.

Russia's invasion of Ukraine has taken place both on and offline, blending physical devastation with escalating digital warfare. Ransomware gangs and other hacking groups have taken to social media to announce where their allegiances lie.

The Record will be tracking who these groups align with, as well as any attacks they launch related to the conflict.

Many of the pronouncements from these groups include threats against critical government infrastructure. Some collectives are state-sponsored while others are decentralized — but all are able to take down computer systems and breach organizations.

"It is now an inevitable part of any military action that so-called 'Cyber Patriots' will engage the perceived enemy either of their own free will or at the direction of their government. Some of these activities, such as Anonymous launching DDoS attacks, will be nothing more than minor nuisances but others could have real consequences," said Allan Liska, a ransomware expert at Recorded Future. "Ransomware groups, for example, have more targets than they can go after right now and may decide to focus on attacking the enemies of their country to create real disruption. And the more skilled groups can have an even greater impact."

Liska warned that Sandworm and UNC1151 are the most concerning in terms of their capabilities and activity, and should be closely monitored.

Siding with Ukraine

Anonymous – United with Ukraine and "officially in a cyber war against the Russian government." The group later tweeted that they targeted Russian-state controlled international television network RT, and "has taken down the website of the #Russian propaganda station RT News." Anonymous is said to be a decentralized hacktivist group that targets different government institutions and government agencies, corporations, and the Church of Scientology. GNG, a hacking group affiliated with Anonymous, has gained access to SberBANK database and leaked hundreds of data files. Sberbank, Russia's biggest lender, is now facing failure. NB65 is another affiliate of Anonymous who Tweeted their support for Ukraine: "#Anonymous is not alone. NB65 has officially declared cyber war on Russia as well. You want to invade Ukraine? Good. Face resistance from the entire world. #UkraineWar All of us are watching. All of us are fighting."

As of February 28th, another group under the Anonymous umbrella named DeepNetAnon has joined in the operations against Russia by attacking and intercepting Russian radio receivers. "The Russians have now taken offline the second web server hosting a Software-Defined Radio receiver (used to interact with Radio Frequencies). Too bad there's many more sites we can use. (;" the group tweeted. The collective also announced that they have successfully hacked the Ministry of Economic Development of Russia. 1LevelCrew also showed their support for Ukraine and tweeted, "TANGO DOWN – http://pfr.gov.ru – Pension Fund of Russian offline. | #OpRussia #Anonymous." Another collective known as HydraUG made a clear statement via Twitter: "Im not here to deface/destroy your website, im here to liberate Ukraine."

> The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine
>
> — Anonymous (@YourAnonOne) February 24, 2022

As of Wednesday, another affiliate named N3UR0515 took to Twitter to share support and call on YouTube to take down Russian propaganda. The group has administered DDoS attacks and taken down 'ria.ru' — the Official Russian Information Website. Joining the Anonymous collective, v0g3lSec announced that they had hacked into the Russian Space Research Institute database and leaked files from Roscosmos, though the hack has not been confirmed.

Ghostsec – Announced their support for Ukraine today: "In support of the people in Ukraine WE STAND BY YOU!" Also known as Ghost Security, the group considers itself a 'vigilante' group and was initially formed to target ISIS websites that preach Islamic extremism. Ghostsec is also commonly referred to as an offshoot of Anonymous.

IT army of Ukraine – After Ukraine's deputy prime minister and minister for digital transformation Mykhailo Fedorov enacted the volunteer application, over 175,000 people have subscribed. Many have been tasked with distributed denial-of-service attacks against Russian websites including government websites, banks, and energy companies. On February 27, officials also told volunteers to target websites registered in Belarus. Fedorov released the target list.

AgainstTheWest (ATW) – Standing with Ukraine, the group's Twitter account says, "We're back in action. Standing against Russia. Active until Russia stands down." The group is actively working to breach Russian infrastructure including Russian railways and Russian Government contractor "promen48[.]ru." As of March 1, the group has issued a new statement for further clarification, "we won't be collaborating with anonymous." Furthermore, "ATW will be splitting into two groups. One for Russia related breaches, one for Chinese related," the group states. ATW accused Anonymous of taking the credit for the work done by ATW: "Anonymous has had a lot of media publicity over the years for hacking, and to see this. It didn't sit right." ATW seems to have been suspended from Twitter as of March 3.

SHDWsec – Joins the movement to support Ukraine. The group is working in collaboration with ATW and Anonymous in operations against Russia, "SHDWSec joined forces with @AgainstTheWest_ First stage is now on the roll. Expecting us is too late. Brace for impact. More to come."

Belarusian Cyber Partisans – Supporting Ukraine. The activist hacking group successfully accessed the computers that control the Belarusian train system, stopping trains in Minsk and Orsha, as well as in the town of Osipovichi. The operation was intended to "slow down the transfer" of Belarus-based Russian troops into Ukraine. Over the past year, the hacktivists have worked against the Belarus government and were able to leak data of secret police archives, lists of alleged police informants, personal information about top government officials and spies, and more.

KelvinSecurity – Announced they stand with Ukraine: "I want to release this to support the digital war against RUSSIA. I have a list of weapons development documents that I took from a Russian ballistic institute and I also have internal videos from RT, and the Russian nuclear institute," the statement says. The group has been tweeting evidence of their engagement in cyber operations.

Raidforums Admin – Stands with Ukraine. The group announced: "Raidforums2 is in support of Ukraine. Members are actively DDOS Russian websites and attacking Russian infrastructure. We also have reason to believe the Chinese are hacking Ukrainian networks." Previously labeled as Raidforum, the collective is now operating as Raidforum2 after having outage and access issues. It is unclear what went wrong with the original Raidforum.

ContiLeaks – Backing Ukraine. The group has exposed infamous ransomware group Conti from the inside out. Since February 27, following Conti's statement of Russian support, an account named ContiLeaks leaked hundreds of files containing internal Conti communications. The informant is believed to be Ukrainian and has continued to leak more and more files as days go by. A more recent data set shows communication depicting the chaos within Conti. Actor 1 says, "Hi, all VM farms are cleared and deleted, servers are disabled." Actor 2 responds, "I deleted all the farms with the shredder and shut down the servers."

Secjuice – Stands with Ukraine. This collective is taking a less volatile approach by using open-source intelligence (OSINT) and psychological operations (PsyOps). At the request of IT army, they are creating a website for missing persons within Ukraine as a resource for families. In a tweet on March 2, the group asked for assistance in ensuring the website is hosted on a safe server and not vulnerable to attacks.

Siding with Russia

Conti – In full support of Russia — "If anybody 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," Emsisoft ransomware expert Brett Callow shared in a tweet. The Conti ransomware gang is highly sophisticated and known for being the first group to weaponize the Log4Shell vulnerability and operate a fully-developed attack chain. Days after Conti ransomware group announced their support for Russia, an insider who is believed to be Ukrainian, leaked 400 files of internal communications between members of the group. The leaked messages go back to January 2021. The data was shared with the malware research group VX-Underground. The hacking collective leaking Conti information is now being referred to as ContiLeaks.

> The Conti #ransomware operation sides with Russia and threatens attacks on critical infrastructure. pic.twitter.com/L8E7IEW1MJ
>
> — Brett Callow (@BrettCallow) February 25, 2022

Minsk-based group 'UNC1151' – Support lies with Russia. The hacking group is commonly regarded as being state-sponsored by Belarus and has already been working to compromise the email accounts of Ukrainian military personnel. The group's "'members are officers of the Ministry of Defence of the Republic of Belarus,' Ukrainian officials added," as reported by The Record. Facebook (or Meta) has taken down accounts used by UNC1151 which targeted Ukrainian officials through Facebook posts that displayed videos that depicted Ukrainian soldiers as weak. The platform also blocked various phishing domains that were being used to jeopardize Ukrainian accounts.

Zatoichi – Supports Russia through the spread of disinformation via the group's Twitter account. Amongst many false claims, the account stated, "Killnet has already put down the Anonymous website, which announced the start of a cyber war with the Russian government, the Right Sector website, and the website of the President of Ukraine."

Killnet — Stands with Russia. The group published a video addressing the people of Russia encouraging them to never doubt their country. The video features a hooded figure with a distorted voice claiming to have taken down the website belonging to Anonymous. Little is known about the group and it is unclear as to whether the group existed previously.

XakNet — Backing Russia. The collective called itself a "team of Russian patriots" in a recent statement and criticized Anonymous, "We do not hide behind the mask of abstract 'Anonymous'." The announcement concludes with a final threat, "For every hack/ddos in our country, similar incidents will occur in Ukraine."

Stormous Ransomware – The collective stands with Russia after they publicly announced, "The STORMOUS team has officially announced its support for the Russian governments. And if any party in different parts of the world decides to organize a cyber-attack or cyber-attacks against Russia, we will be in the right direction and will make all our efforts to abandon the supplication of the West, especially the infrastructure. Perhaps the hacking operation that our team carried out for the government of Ukraine and a Ukrainian airline was just a simple operation but what is coming will be bigger!!" The group has been around since the beginning of 2022 and is believed to be financially motivated. Their messages are in Arabic. More recently on March 1, the group issued a warning against "western unions" and more specifically companies in the U.S., after being attacked by unspecified U.S. companies causing their site to be shut down.

Digital Cobra Gang (DCG) – Supports Russia. Another group has stated their allegiance with Russia in a public statement that reads, "DIGITAL COBRA GANG DCG has officially declared cyber war on hackers who attacking Russia as well and to protect justice. Do you want to invade Russia? Taste the good from the whole WORLD #Ukrainewar #Russia We fight for the Good, 10m deaths and 50 wars Russia? NO!" The group entered the cyber war via Twitter on February 27th. The most recent update declares their use of a 'secret weapon.' "We set many traps so we have wired 27.918 computers from the guys who attacking Russia and we are ready to drop our secret weapon."

Freecivilian – United with Russia. The group is reportedly advertising stolen data from 50 different Ukrainian government websites from a February 23 attack. The attacks on the websites included displayed defacement messages that were almost identical to messages from a January 15 attack linked to UNC1151. Although claiming to be an independent cybercriminal, many suspect the group is linked to nation-state actors.

SandWorm – Backed by Russia. The group, known for its recent malware called Cyclops Blinks, is comprised of Russian state-sponsored hackers. The malware was first deployed in June 2019 and "has been primarily detected targeting WatchGuard Firebox firewalls, but they don't exclude having the ability to infect other types of networking equipment too," Catalin Cimpanu reported for The Record.

The Red Bandits – Stands with Russia. On February 22, the group tweeted, "We've hijacked the @UkrainePolice Dashcams and have been watching them. If Ukraine does not do what #Russia wants we will escalate our attacks against Ukraine to involve panic scares. We will also consider distributing #ransomeware in #UkraineRussiaCrisis #RussiaUcraina #Ukraine." The collective self-identifies as a cybercrime group from Russia, however, it is widely speculated to in fact be Russian Intelligence.

Since their original statement, the group seems to be wavering in its threats against Ukraine. The group tweeted on March 1: "We want everyone from #Ukraine to read this: We stand strongly with citizens of #Ukraine and that's why we have not attacked anything other than their government. We also have not given a percentage of intel we have against Ukraine," the tweet continues in a long thread. "We do not respect Putin as a #leader of #Russia but we respect him as a citizen of #Russia as we support every citizen. We do not agree with his unpeaceful actions against #Ukraine as an operation." The statement continues in a later post, "Please understand, we're not going to stop defending our country. We will not surrender because of reasons but we will not attack first, we'll defend attack meaning you guys hack Russia a few times we hack back. Simple, please understand we see #Ukraine citizens as family."

The group's messages have become increasingly ambiguous and ominous, and they tweeted — hours after claiming to be family with Ukrainians — a job application for those experienced with breaching networks. On Wednesday, March 2 they tweeted, "We seen a chance to make millions, we're going to take that chance."

> We've hijacked the @UkrainePolice Dashcams and have been watching them. If Ukraine does not do what #Russia wants we will escalate our attacks against Ukraine to involve panic scares. We will also consider distributing #ransomeware in #UkraineRussiaCrisis #RussiaUcraina #Ukraine pic.twitter.com/zEgtZxzDqP
>
> — TheRedBanditsRU (@RedBanditsRU) February 22, 2022

Coomingproject – Sides with Russia. The international hacker group announced today in a statement, "Hello everyone this is a message we will help the Russian government if cyber attacks and conduct against Russia." The gang is linked to the 2021 data breach and leak of the South African National Space Agency.

The domino effect of hacker announcements prompted Ukraine's Defense Ministry to send a message to the Ukrainian underground hacker community. The message was a call-to-action encouraging Ukrainian hackers to assemble in a mission to protect the nation's critical infrastructure from cyberattacks and act offensively against Russia in cyber espionage operations. Although requested by the Defense Ministry, the message was published by Yegor Aushev, the founder of Cyber Unit Technologies, who provided an application for those in the hacker community to apply.

Emma Vail is an editorial intern for The Record. She is currently studying anthropology and women, gender, and sexuality at Northeastern University. After creating her own blog in 2018, she decided to pursue journalism and further her experience by joining the team.