

Russia-Ukraine Conflict: Situational Updates

ZEROFOX INTELLIGENCE BRIEF

B-2022-0303a

Classification: White

Criticality: High

Intelligence Requirements: Geopolitical & Physical, Malware, Deep Dark
Web & Criminal Underground

CI

March 3, 2022

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on March 3, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Executive Summary

Despite suffering setbacks from pushback by a determined Ukrainian military and stiffer Western response than anticipated, Russia's military escalation in Ukraine is unlikely to end soon, as Russia's primary focus remains decapitating the current Ukrainian government.

Key Findings

- The Russian military escalation is largely being fought on four fronts and is proceeding more slowly than anticipated.
- The Ukrainian military response has been more robust than Russia anticipated, and the international response has been more aggressive than initially forecasted.
- Despite the military setbacks, forced regime change remains Russia's priority, which will see the Ukrainian capital and largest city of Kiev engulfed in conflict.
- Despite early speculation that ransomware groups would begin voicing their support for the Russian government, most groups have long claimed to be politically neutral and interested only in financial gain. However, after initially expressing support for Russia and then walking back its statements, the Conti ransomware group experienced a very public downfall in the past week.

Details

Geopolitical Impacts

The Russian military has made slower progress than anticipated in its invasion of Ukraine. A combination of poor planning and logistical support, unrealistic expectations, and unexpectedly fierce Ukrainian resistance has held up the Russian advance and resulted in much higher-than-expected casualties. The envelopment of the capital Kyiv and a forced regime change remains Russian President Vladimir Putin's primary objective, but it is probable that he expected a quick strike on Kiev with little resistance that would be completed within one to three days. Russian propaganda also suggests that its leaders may have expected to be greeted as liberators in some Ukrainian cities.

Despite Ukraine's determined military opposition and President Volodymyr Zelensky's effective appeals for international support, the military situation has deteriorated. Russian forces have maintained consistently brutal shelling of Kharkiv and gained control of Kherson, northwest of Crimea. Mariupol is reportedly surrounded and without water and electricity. A massive convoy, which satellite company Maxar Technologies estimates is 40 miles long, of Russian troop transport, artillery, and logistical support vehicles is waiting northwest of Kyiv. The convoy is temporarily stalled but may be awaiting the approach of troops near Bobrovytsya to the east to help encircle and besiege the capital. U.S. officials have also stated that they expect heavier bombardment and greater manpower directed at Ukraine's major cities in the coming days.¹

The United Nations (UN) estimates that one million refugees have already fled Ukraine since the start of the war, but the next weeks may create the conditions for a much larger humanitarian catastrophe. Civilians in Kyiv and Odesa will likely face conditions similar to those currently taking place in Kharkiv, Mariupol, and the other besieged cities. Russia reportedly intends to create humanitarian corridors exiting the surrounding urban centers, but it is unclear what form that will take and who will be allowed to pass. A humanitarian disaster may already be underway in Mariupol. Mariupol's deputy mayor told CNN that the city is surrounded and waiting for military help without water, electricity, or heat.²

¹

<https://www.cnn.com/videos/world/2022/03/01/russian-military-convoy-more-than-40-miles-long-sciutto-intl-ac360-dnt-vpx.cnn>

²

https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-03-22/h_bb7d246bf72ba79f73edf9464f2b3712



Source: <https://www.ft.com/content/575cba8a-4b1f-411b-84f3-3b5afe2202e3>

Absent an unexpected change in Russian strategy, such as the withdrawal of troops from contested regions, it is unlikely that ongoing peace negotiations will yield significant results. Representatives from Russia and Ukraine met on the Ukraine-Belarus border on February 28, 2022, for the first round of ceasefire negotiations since the Russian invasion commenced on February 24, 2022. Initial talks were inconclusive, but the second round of talks reportedly began on March 3, 2022. However, Russia's coordinated approach to the talks suggested that they were not treated as a legitimate opportunity to peacefully conclude the conflict. Russia fired missiles at Ukraine as the negotiations were ongoing, and Russia's lead delegate was a former Minister of Culture instead of a senior foreign affairs or defense official. President Putin also told French President Emmanuel Macron on March 3, 2022, that Russia's operation objectives "will be achieved whatever happens."

The Ukrainian government's posture also indicates that it does not expect the war to end soon. In calls with the European Parliament and U.S. President Joe Biden, Ukrainian President Volodymyr Zelensky has urged the European Union (EU) and the United States to help more and impose greater costs on Russia. CNN interviewed President Zelensky from his Kyiv bunker on March 1, 2022, during which he said President Biden should give a "useful" message to the people of Ukraine during his State of the Union address.

International Response and Sanctions

The international response to the crisis was both swifter and more aggressive than events prior to the invasion suggested. The EU and the United States quickly implemented sanctions targeting Russian banks and individuals close to President Putin, Germany ended the certification process for the Nord Stream 2 pipeline, and the EU announced on March 2, 2022, that it was blocking seven Russian banks from the SWIFT payment messaging system. Switzerland surprisingly broke with its history of neutrality to freeze Russian assets and impose EU sanctions. During his State of the Union address, President Biden announced that the United States would close its airspace to Russian aircraft, mirroring a move that the EU had made days prior. Western leaders have thus far avoided proposals to introduce oil and gas embargoes, as they could further exacerbate unprecedented energy prices and supply deficiencies. However, that may soon be changing in the United States, as Senators Joe Manchin and Lisa Murkowski are expected to introduce a bill on March 3, 2022, that would ban imports of Russian oil. Speaker of the House of Representatives Nancy Pelosi is also reportedly in favor of adopting a ban on Russian oil imports and is pressuring the Biden White House to support it.³

Western countries have also increased weapons deliveries to Ukraine. The United States reportedly delivered 200 Stinger air defense systems to Ukraine for the first time on March 1, 2022, with further shipments of Stingers and anti-tank Javelin missiles expected. In another historic reversal of precedent, Germany announced that it would send millions of weapons to Ukraine, including 1,000 Panzerfaust 3 light anti-tank weapons and 500 Stingers. The United Kingdom, Sweden, and Finland have each sent thousands of anti-tank weapons.⁴

Many large corporations responded to the conflict by cutting off relations with Russia. In the oil and gas sector, BP, Shell, Exxon, and Equinor have begun the process of withdrawing from their Russian partnerships. FedEx and UPS announced the suspension of shipments to Russia, Delta said that it would no longer partner with Russian state airline Aeroflot on flights, and Apple halted its product sales in Russia. IKEA also said that it would stop its operations in Belarus and Russia. The Russian government has attempted to head off the worst effects of the sanctions by applying their own financial safety measures, but the value of the ruble has already fallen below RUB 100 per dollar.

³ <https://www.ft.com/content/d998aa88-d06c-4352-beda-45e82ed8052e>

⁴

<https://www.popularmechanics.com/military/weapons/a39281936/weapons-europe-is-sending-to-ukraine/>

Russians will undoubtedly suffer under Western sanctions, but sanctions alone are unlikely to deter President Putin from seeking to oust President Zelensky and occupy Ukraine. High casualty figures and the collapse of the ruble will put immense domestic pressure on President Putin, even if he introduces martial law on March 4, 2022, in Ukraine as Oleksiy Danilov, Secretary of the National Security and Defense Council of Ukraine, has claimed is likely.⁵ Putin is seeking re-election in 2024 and will need military success to justify the costs of facing down the West and to demonstrate to the Kremlin that he remains the singular figure of authority. Additionally, President Putin has judged that NATO intervention in the war is very unlikely. President Zelensky has pleaded for NATO to impose a no-fly zone over Ukraine, but that would, by definition, lead to a hot war with Russia. President Biden and other European leaders will not take the risk of expanding the conflict and increasing the chances of nuclear war.

Physical Security Impacts

The Russian military is broadly advancing along four fronts: from Crimea in the south, where they have targeted Kherson and Mykolaiv; through the occupied Donetsk and Luhansk territories in the southeast, where troops have enveloped Mariupol; through the northeast, to Kharkiv and Sumy; and from Russian and Belarusian territory in the north to advance on Kyiv. Rather than bypass urban areas to minimize casualties and focus forces on Kyiv, the Russian military has targeted all major cities east of the Dnieper river. The fiercest fighting appears to be taking place in Mariupol and Mykolaiv in the south and in Kharkiv.

On March 2, 2022, Kherson became the first major Ukrainian city to fall to the Russian military. The city's mayor told *The New York Times* that he met with a Russian commander who plans to set up a military administration in the city. Closed-circuit video from Kherson showed Russian forces with prisoner transport vehicles occupying Freedom Square in the Kherson city center. The revelation that Russia plans to set up local governments in overrun cities suggests more extensive plans for the military occupation of Ukraine.⁶

Kharkiv has thus far been the Ukrainian city hit hardest by Russian missile strikes. On March 1, 2022, a 3M14 Kalibr land-attack cruise missile struck the city's administrative building and resulted in 10 deaths, according to local authorities. Later in the same day, Russian paratroopers landed in the city. President Zelensky has called the strikes on Kharkiv—which Ukraine alleges are targeting civilian

5

<https://www.ukrinform.net/rubric-ato/3418415-on-march-4-russia-set-to-impose-martial-law-ukraines-nsdc-secretary.html>

⁶ <https://www.nytimes.com/2022/03/02/world/europe/kherson-ukraine-russia.html>

population centers—evidence of war crimes.⁷ Kharkiv’s destruction and capitulation is likely one of President Putin’s foremost current objectives. As a border city with a majority of Russian speakers, the city was symbolic of Russia’s initial military mission to “liberate” Ukrainians. Its determined resistance speaks poorly of Russian strategy, and Kharkiv will continue to face an intense onslaught.

U.S. officials expect that the attack on Kyiv will commence in the next few days. The Russian military will likely attempt to surround the city with forces from the east and introduce the massive convoy stationed to the city’s northwest. Kyiv may then face a bombardment similar to the one on Kharkiv that results in large numbers of civilian casualties. According to Ukrainian intelligence, Russia has attempted to strike at President Zelensky in other ways. Secretary Danilov alleged that a squad of Russian mercenaries was “neutralized” in the capital during a mission to assassinate the president.⁸

Odesa will be the next city to face concerted Russian firepower. Russian naval vessels have gathered off the coast and will likely attempt to link with forces coming from Mykolaiv to the northeast. With Crimea occupied and Mariupol under siege, Odesa is Ukraine’s last major port to be relatively untouched by the war. It is also the final significant obstacle to creating a land-bridge from Russia through Crimea to Ukraine’s Black Sea coast and would thus cut Ukraine off from its access to the sea.

The next phase of the war will likely depend on Russia’s success in Kharkiv, Kyiv, and Odesa. If Russian forces have success overrunning Kyiv and Kharkiv, they will likely advance on Dnipro, in the center of the country, and may approach from four directions. This move would allow the Russian military to separate east and west Ukraine—and perhaps renew negotiations with the West after having taken control of the Black Sea coast, destroyed Kyiv, and occupied the eastern half of the country. However, to date Russian losses have far exceeded initial expectations. The General Staff of the Ukrainian Armed Forces estimates over 9,000 Russian casualties and more than 1,500 vehicles lost. While these may be overestimates, it is clear that Russian losses have been significant. If the attacks on Kyiv and Odesa prove much more costly than anticipated, or drag on for weeks, President Putin’s calculus regarding further advances may change. Nevertheless, Western officials currently believe that he intends to take control of all of Ukraine.

7

<https://defense-blog.com/bellingcat-identified-missile-that-russia-used-to-strike-on-kharkiv/>

8

<https://www.thetimes.co.uk/article/volodymyr-zelensky-russian-mercenaries-ordered-to-kill-ukraine-president-cvcksh79d>

Cyber Impacts

On February 27, 2022, just two days after the Conti ransomware group seemingly pledged (and later walked back) their support to the Russian government, a new Twitter account shared a link to download alleged chat logs from the Conti ransomware group. The ContiLeaks account has tweeted several times since then, sharing information on members of the group, its infrastructure, documentation, and even full source code. The downloaded zip file containing Conti's full source code was password protected, however. While the password for this file was not shared publicly, ContiLeaks shared a second source code file with the encryption removed.



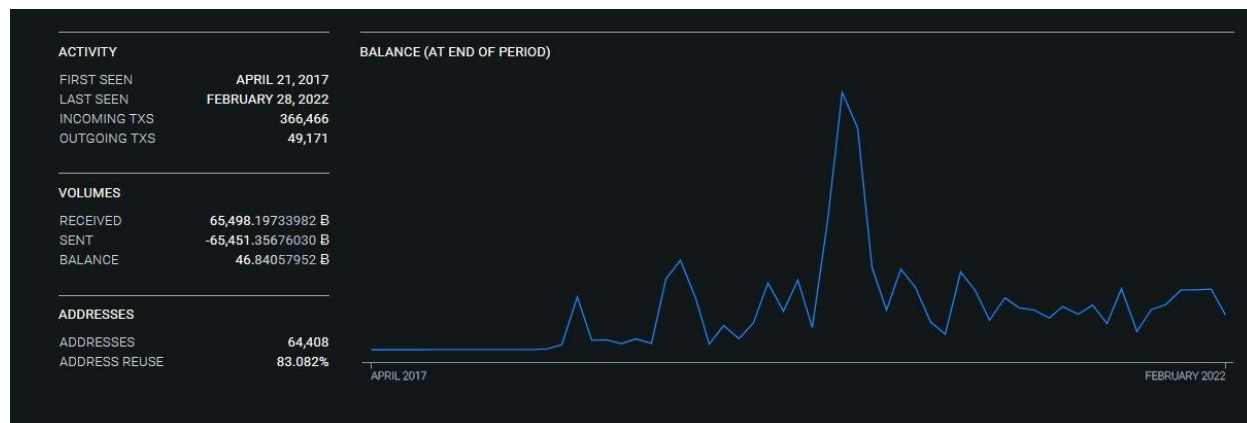
Source: ZeroFox Intelligence

There has been debate as to whether or not the source of the leaks was a Ukrainian affiliate, a member of the group, or a security researcher.⁹ Whatever the case, the sentiment in tweets by ContiLeaks suggests that the individual supports Ukraine, which could have led to their decision to begin leaking data even though Conti quickly removed and revised their statement supporting Russia.

Many researchers have begun dissecting the leaked chat logs, translating them and searching for any useful information they can find. One of the more interesting things to surface so far is a claim that Conti's Bitcoin wallet address has been discovered. From April 21, 2017, through February 28, 2022, the address received

⁹ <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>

over 65,000 BTC. Initial statements estimated this to be worth more than USD 2.7 billion but did not take into account changes in value over time, instead using the current USD exchange rate for all transactions. In addition to discovering Bitcoin wallets, chat logs could potentially reveal previously unknown victims.



Source: <https://twitter.com/vxunderground/status/1498394338027610124/photo/1>

Leaked source code can be a double-edged sword. While it provides security researchers with an excellent opportunity to study the code for any vulnerabilities with the encryption implementation, this also means that the code is available to cybercriminals looking to use it as well. ZeroFox has already seen this to be the case with now-defunct ransomware groups, such as Babuk, having their source code leaked.¹⁰

Conti's decision to quickly revise their statement supporting the Russian government is important to note. Most ransomware groups claim political neutrality and that money is their only goal. Very few previously-tracked threat actors and groups have publicly voiced support for Russia so far. Conti's very public downfall may give other actors pause for thought before making pledges to support any one nation's government.

After the leaks became widespread, Conti reportedly wiped their servers.¹¹ Although ransomware groups are known to disappear and rebrand at times like this, it is currently too early to know how this will affect the group's operations.

¹⁰ <https://www.zerofox.com/blog/babuk-ransomware-variant-delta-plus/>

¹¹ <https://twitter.com/radvadva/status/1499100075859103748>