POINT OF VIEW

Recorded Future®

By John Wetzel

January 27, 2022

Russia's Biggest Threat Is Its Instability

Executive Summary

- Due to domestic concerns over the last 2 years, as well as perceived external threats, The Kremlin likely seeks to deflect attention away from these troubles by employing state-sponsored cyber assets, military pressure, and allied governments who can be brought to bear on targets of strategic interest to Russia. This serves the dual purpose of also signaling to NATO nations that Russia is unwilling to accept the further encroachment of NATO nations on its borders, especially Ukraine and Georgia.
- The false flag defacement attacks on Ukrainian websites were tied to Belarusian entities but with benefits to Russian strategic objectives.
- The Kremlin remains a dangerous source of global geo-cyber instability precisely because of its willingness, at times, to deviate from formal doctrine to improvisation when engaging in direct military action—Russia has accelerated the weaponization of confusion and provocation to create a multi-state standoff centered around Ukraine, to thwart NATO expansionary pressures.

Russia Accelerates Aggression Towards Ukraine

The Kremlin is a complex actor within both the geopolitical and cyber domains. Since the 2014 Maidan revolution which led to the fall of the Ukrainian government of Victor Yanukovych and resulted in the Russian military invasion of Crimea, Russia has accelerated military force, influence operations, and cyber capabilities towards Ukraine. Yet rather than directly engage in military invasion, Russia has leveraged elements of "active measures"–subterfuge, indirect action, and cyber campaigns–complicating analysis and clouding insight. In this article, we explore and clarify the last few weeks of activity within Russia, Ukraine, and Kazakhstan, looking at three domains: diplomatic and military actions, cyber offensive actions, and traditional espionage.

Starting March 2021 and surging late last year, Russia has accelerated regional tensions through a series of aggressive actions mainly directed against Ukraine. At present, Russia has marshaled approximately 100,000 troops and support units near the Ukraine border, representing around 35% of its total battle groups. The troop surge has drawn considerable consternation from NATO members, which has placed its own troops on increased operational alert.

Some European countries, like Germany and the UK, have publicly denounced Russian actions and warned of serious consequences for Russia should an invasion against Ukraine take place. During a press briefing on November 15, 2021, NATO Secretary-General Jens Stoltenberg warned of a "significant, large Russian military build-up, along the Russian/Ukrainian border", and noted that NATO is monitoring the situation. On November 20, 2021, Ukraine's defense intelligence chief Kyrylo Budanov stated that Russia "is preparing for an attack by the end of January or beginning of February". The United States has supported NATO allies, reportedly negotiating with Germany to halt the completion of the Nord Stream 2 pipeline if Russia invades Ukraine, and also weighing the removal of Russia from the SWIFT banking system in a sanctions package. Russian President Vladimir Putin responded on December 9, calling the ongoing conflict in Donbas a "genocide" during a meeting of the Presidential Human Rights Council.1 Still, the United States and the United Kingdom have stated they will not be deploying troops to Ukraine. On January 22, 2022, the United Kingdom Foreign Secretary issued a statement stating that it has information that Russian intends to install a pro-Russian leader for Ukraine as it considers invasion. According to the statement, the former Ukrainian MP Yevhen Murayev is being considered as a potential candidate. Additionally, the statement claims, "We have information that the Russian intelligence services maintain links with numerous former Ukrainian politicians including:

- Serhiy Arbuzov, First Deputy Prime Minister of Ukraine from 2012-2014, and acting Prime Minister in 2014
- Andriy Kluyev, First Deputy Prime Minister from 2010-2012 and Chief of Staff to former Ukrainian President Yanukovich
- Vladimir Sivkovich, former Deputy Head of the Ukrainian National Security and Defence Council (RNBO)
- Mykola Azarov, Prime Minister of Ukraine from 2010-2014"

Russian Espionage May Enable Pretext for Ukraine Invasion

Adding to the regional chaos, increasing Russian government espionage, planned sabotage, and information operations can act as a force multiplier for any pretext for war.

- In October 2021, NATO expelled Russian diplomats in Brussels due to alleged espionage activities, and Russia responded by closing its entire NATO embassy.
- On December 2, 2021, the Russian Federal Security Service (FSB) announced the arrest of "3 Ukrainian spies" who were purportedly plotting acts of terrorism.
- Recorded Future's Insikt Group tracked a viral claim posted on Russian social media website Odnoklassniki in December 2021 claiming that Ukrainian soldiers, allegedly "left without food" are stealing livestock from residents in Donbas.
- On December 14, 2021, the Russian Mission to the United Nations (UN) denounced a Ukrainian "water blockade" on the Crimean Peninsula, claiming that this behavior has limited Crimeans' access to safe and sanitary drinking water.
- On December 21, Russian Minister of Defence Sergei Shoigu, stated that a US private military company is preparing a provocative action using an unidentified chemical weapon which was allegedly delivered to Avdiivka and Krasnyi Lyman, Donbas.
- On Monday, January 10, 2022, the Security Service of Ukraine (SBU) announced, that it had detained an alleged Russian military intelligence agent, stating that the individual was in process of planning a series of terror attacks near the port of Odessa.
- Subsequently on January 14, 2022, US officials accused Russia of sending saboteurs into eastern Ukraine in order to create pretext for an invasion.

While giving plausible deniability to Russian officials, these claims and subversive acts work together to foment domestic distrust of Ukraine and potentially set the stage for further action. What is less deniable are the measures that Russian military forces are preparing for action, including publicizing a video on November 29, 2021, showing a RS-24 Yars intercontinental ballistic missile (ICBM) being loaded into a silo at the 28th Guards Missile Division Kozelsk Missile Base in Kaluga Oblast.

1 http://en.kremlin.ru/events/president/news/67331

Ukrainian Government Websites Defaced, and Suffers Additional Destructive Cyber Attack

In apparent coordination with Russian diplomatic and military aggressions, cyber activity against Ukraine has increased in recent days, including a false flag defacement and destructive attack against Ukrainian organizations. On the night between January 13 and January 14 2021, threat actors defaced the websites of the Ukrainian Ministry of Foreign Affairs, Ministry of Education and Science, Ministry of Defense, the State Emergency Service, the website for the Cabinet of Ministers, and others. According to The Record, all website data was wiped and a message was posted stating the following: "Ukrainian! All your personal data has been sent to a public network. All data on your computer is destroyed and cannot be recovered. All information about you stab (public, fairy tale and wait for the worst. It is for you for your past, the future and the future. For Volhynia, OUN UPA, Galicia, Poland and historical areas".

Ukrainian officials attributed the attack to Belarusian intelligence. On January 14, 2022, Ukrainian CERT issued a statement regarding the attack, and noted in addition to the website defacement, there was a coinciding destructive wiper and corrupter attack on Ukrainian networks. Ukrainian CERT described preliminary analysis that determined the likely attack vector for the website defacement was a known vulnerability in the October CMS web content management platform, CVE-2021-32648. Though the scope of the Ukrainian CERT analysis focused on the October CMS, Ukrainian SBU analysis shows this may have been one part of a wider attack against a hosting provider. The defacement included a message as an image file and was posted in Ukrainian, Russian, and Polish languages, and included metadata with the following coordinates: Latitude: 52° 12′ 31.1″ N, Longitude: 21° 0′ 33.9″ E, GPS position: 52.208630, 21.009427, which is the parking lot of the Warsaw School of Economics. As noted by the Polish Ministry of Defense CSIRT, the image used in the defacements is not a photograph, so the image metadata was likely added manually. Additionally, open source commentators noted errors in the Polish language text, with the Polish government issuing a statement suggesting that the content was likely not written by a native Polish speaker.

Ukrainian authorities attributed the website defacement attack to UNC1151, a threat activity group linked by Mandiant to the Belarusian government, and which has also been associated with the Ghostwriter campaign. Previous attacks in this campaign have targeted Lithuania, Latvia, and Poland with "narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe". In September 2021, UNC1151 was blamed for temporarily disrupting the websites belonging to the authority managing Germany's General Election. UNC1151 appears to leverage credential harvesting as an initial entry vector. While some early speculation placed blame directly on Russian entities, when Ukraine blamed UNC1151 many news outlets reported on the ties to Belarus. As noted above, previous reporting did tentatively tie UNC1151 to Belarus, though Germany maintains likely Russian involvement with UNC1151. Attribution has interesting implications here. If Belarus is behind the activity targeting Ukraine, Silverado Policy Accelerator founder Dmitri Alperovitch points out this may indicate Belarus has decided to support a potential Russian campaign against Ukraine. Further investigation is needed to conclusively identify the culpable actor.

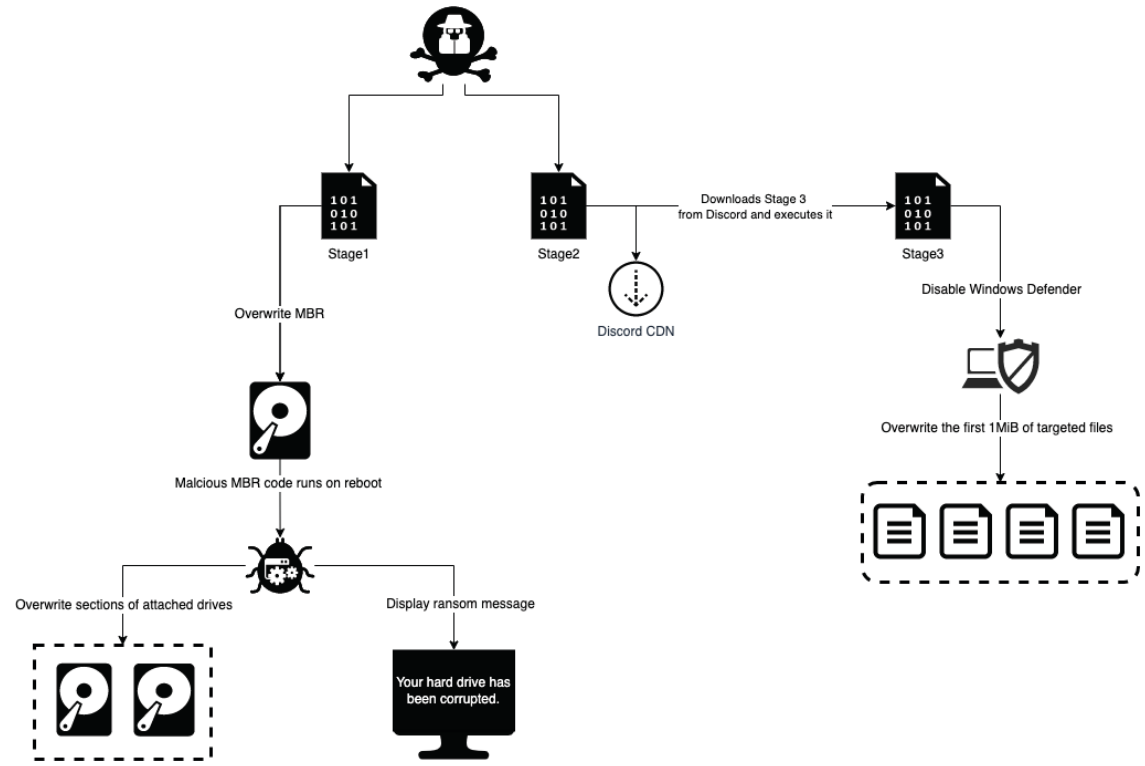

Figure 1: Stages of WhisperGate malware (Source: Recorded Future)

In addition to the website defacement, a destructive wiper attack posing as ransomware targeted Ukrainian organizations. On January 15, Microsoft published a blog covering the destructive malware, which they named WhisperGate and attributed to DEV-0586, an as-of-yet unattributed threat actor. Microsoft stated this attack spanned "multiple government, non-profit, and information technology organizations, all based in Ukraine", indicating broader targeting than the government website defacement. As described by Microsoft, WhisperGate malware uses three stages, functionally named stage1[.]exe, stage2[.]exe, and a third stage downloaded from a Discord server as a .jpg file. On Sunday, January 16, Microsoft submitted the files into file analyzer service VirusTotal. The malware overwrites a hard disk's Master Boot Record (MBR) with no recovery option, corrupts a number of files based on file extension, and displays a fake ransom message (in that no ransom can actually be paid to recover the files) requesting payment of $10,000 USD to a Bitcoin address, 1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv. Microsoft noted this Bitcoin wallet address is consistent across all DEV-0586 intrusions and appears to only have a single small transfer on January 14.

Other Russian-Nexus Cyber Activity Occurring

Interestingly, the Ukraine defacement activity is not the only recently observed activity with a potential Russian nexus. Google Threat Analysis Group detected ongoing APT28-related credential phishing campaigns targeting Ukraine, which appears to be independent from the website defacements. Domains reported are:

- consumerpanel.eu3[.]biz
- consumerpanel.eu3[.]org
- consumerspanelsrv.eu3[.]org
- protectpanel.eu3[.]biz
- updateservicecenter.blogspot[.]com

Meanwhile Russian-affiliated ransomware actors continue to operate, albeit with an apparent nod towards consequences. On January 14, 2022, Russian Federal Security Service (FSB) raided and shut down the operations of the REvil ransomware gang. According to news reports, raids were conducted at 25 residences owned by 14 members suspected to be part of the REvil team across Moscow, St. Petersburg, and the Leningrad Oblast and Lipetsk Oblast regions. Subsequent to the arrests, the Biden administration says one of the arrested members was responsible for the May 2021 Colonial Pipeline attack. Analysts tracking ransomware gang conversations on closed forums have stated that actors believe "this arrest was a publicity operation aimed at a formal public demonstration of Russia's political intent to cooperate" with United States-led negotiations. Yet there is the strong possibility that this law enforcement action is linked to the tensions in Ukraine–less a good faith action and more a mere feint toward cooperation rather than true change. Somewhat supporting this belief is the fact that REvil gang members were charged under money laundering laws rather than hacking.

Of course, Russian-affiliated ransomware activity has continued. Ransomware is not only a US-problem, as entities globally, across all industry verticals have been impacted. According to the Risky Business Newsletter, "Chinese organizations are routinely being compromised by ransomware", and the bulk of this activity is attributed to Russian-speaking criminal actors. "Chinese security vendors attribute these attacks to a lot of familiar names. Sodinokibi and GandCrab, both associated with REvil, top the list." And Russian law enforcement isn't the only agency targeting ransomware gangs–Ukrainian law enforcement is also continuing to crack down on ransomware activity. Earlier in the week of January 14, 2022, Ukrainian authorities detained five members of a ransomware gang that carried out attacks on more than 50 companies across Europe and the Americas. Since the start of 2021, Ukrainian authorities have arrested members of the Egregor, Cl0p, REvil, LockerGoga, and MegaCortex ransomware gangs.

Kazakhstan Uprising, Invites Russia, Others To Send Troops

Russia's focus on addressing NATO expansion has been further complicated by the January 2022 protests across Kazakhstan. Battling countrywide protests, the government and security forces of Kazakhstan shut down the internet and communications, increased rhetoric and violence against protesters, and formally requested assistance from Russia-aligned nations. Early reports of communications disruptions surfaced on January 2 as Kazakh citizens took to the streets in Almaty and other cities to protest fuel price increases and deteriorating economic conditions, according to The Record. Network monitoring firm Kentik noted the first outage at 4:45 PM local time on January 5, followed by a second disruption early Thursday, January 6, according to NetBlocks. By January 5, Kazakh President Kasym Jomart Tokaev formally requested the assistance of the Collective Security Treaty Organization (CSTO), a military alliance between Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, and Tajikistan. Of these nations, Kyrgyzstan was the last to deploy troops to Kazakhstan. The Russian Ministry of Foreign Affairs labeled the protests in Kazakhstan as a "foreign-inspired attempt to violently undermine the security and integrity" of Kazakhstan.

Analysis

The Russian economy is currently performing poorly, as Russia continues to struggle with another wave of COVID-19 cases, and despite oil prices nearly double the official budget, many infrastructure projects remain delayed. When viewed globally, Russia is a country with a GDP roughly equivalent to Canada, about one third of Germany's GDP, and due to its reliance on exports of oil and gas is prone to market fluctuations. Russia's lackluster response to the COVID-19 pandemic has exacerbated domestic instability and even resulted in violence relating to pandemic public health restrictions, as was the case when a former SVR officer opened fire in Moscow after being asked to don a mask, killing 2. Politically, the Russian government continues to face challenges from opposition groups, despite the fact that the most outspoken opposition leader, Alexei Navalny, remains in prison since early 2021. In October 2021, the Kremlin declared Navalny and his organization as terrorists and extremists, a designation coming the same week Russian journalist Dmitry Muratov was awarded the Nobel Peace Prize for reporting on government corruption and human rights violations in Russia. Russian authorities have engaged in a number of efforts to label prominent independent journalistic outlets and other "undesirable" organizations as "foreign agents", effectively blocking them from operating or receiving funding in Russia. These organizations pose a threat to prevailing Kremlin narratives, some of which seek to reframe the recent past. A prominent example of this "foreign agent" labeling comes in the form of the dissolution of the prestigious Memorial human rights organization in December 2021.

Despite current economic concerns the Russian government has also made significant increases in defense spending and force modernization efforts in recent years, raising spending by 15% in the 2022-2024 budget and increasing spending for security agencies – which include a significant share for intelligence agencies – by 17%. Partially, this can be seen as deflecting internal challenges by focusing on perceived external threats. Russia has also invested heavily in military modernization, including fielding a new Kinzhal hypersonic missile, the development of a nuclear-powered cruise missile, and modernizations of nuclear-powered and nuclear-armed weaponry. The Kremlin has repeatedly referenced Western threats, while insisting on security guarantees from NATO expansion. Yet these defense spending increases come with a significant caveat – Russia's federal budget assumes an annual growth rate of 3%, yet the Russian economy has been stagnant for years.

Economic and domestic realities shape the Russian government's outlook as it shifts troops to the Ukraine border and considers its relationship to NATO. The Kremlin has a clear interest to build stronger allegiances with former Soviet states as a strategic hedge to NATO, notably joint exercises between CSTO members and China. While enjoying close ties historically, the relationship between Belarus and Russia has not always been smooth, with Belarus at times courting European interests as well as Russian - a marked shift has occurred since the contested 2021 Belarusian elections, however, with Belarus more closely aligned to Russia than in previous years. 2021 saw the largest Russian joint military exercise since 2012 occurring in Belarus in the form of the Zapad (West) 2021 exercises, with Russian and Belarusian forces executing a defense against a simulated NATO incursion–and the two nations are starting new military exercises in February. There are additional insights to draw from the Zapad 2021 joint military exercise with Belarus, most notably a shift in Russian strategy to preserving the military force and an emphasis on strategic targets versus sustained combat. As noted Russian scholar Michael Kofman states, "The clearest shift in Russian thinking is away from strategic ground offensives and towards long-range strikes against critically important economic and military targets, seeking to degrade a state's ability or will to sustain a conflict". The shift to strategic targeting to degrade a state's will to sustain a conflict highlights recent efforts by the Kremlin to engage Ukraine on cyber and information domains.

Further complicating issues are the internal politics of Putin's empire. Political opportunists and oligarchs who seek favor with the Kremlin hold incredible power, and may come to play in a Ukrainian invasion. Political opportunists hold power despite never being elected, such as Vladislav Surkov. In a 2014 interview, Vladislav Surkov described himself as, "...the author, or one of the authors, of the new Russian system." Surkov is the former Russian Deputy Chairman and personal advisor to Putin. Though no longer holding official office, Surkov stage-led the Kremlin annexation of Crimea and ongoing conflict eastern Ukraine from 2014. While never elected, Surkov was known as Putin's "Grey Cardinal", and though officially dismissed from his post in 2020, he has continued to influence and promote the Kremlin's agenda, even recently stating, "An overdose of freedom is lethal to a state." On the business side are players like Yevgeny Prigozhin, once called "Putin's Chef" for his catering and restaurant businesses used by the Kremlin for state dinners. Prigozhin's businesses extend from a $3 billion-a-year Kremlin contract for food services to Russian government institutions, to government-backed disinformation campaigns such as the 2016 US election interference campaigns, and paramilitary operations conducted by the Wagner Group, an unincorporated private military company with links to the Russian Ministry of Defense and a history of clandestine operations in Eastern Ukraine, Syria and several African countries. The Wagner Group has been linked to the Russian-backed mercenaries operating in eastern Ukraine. These opportunists serve to muddy the waters of Russian influence and may come into play in a Ukraine invasion.

Employing cyber elements and information campaigns in advance of [or "in place of"] kinetic actions helps the Kremlin maintain deniability and add unpredictability to the ongoing Ukraine conflict. Adding to this confusion are the lack of consensus around Russian actions and strategies such as hybrid warfare. In the 2014 Crimean annexation which occurred in the shadow of the Maidan revolution, some commentators stated relatively few hybrid elements were present; RAND Corporation notes, "The Russian information campaign accompanying its military movements was no more than a minor contributor to what proved to be a conventional takeover". Yet the US Army War College noted a number of cyber and information warfare elements in the invasion of Crimea, including that, "cyberattacks against Crimea shut down the telecommunications infrastructure, disabled major Ukrainian websites, and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula." While some Russian military offensives in Ukraine look less contrived than improvised, Russian views warfare is conducted on all strategic fronts available, military advances coordinated with non-official government organizations such as mercenary forces and disinformation campaigns leading and preparing the way. Yet this coordination can vary in both execution and results–a "Gerasimov doctrine" this is not, and in the Kremlin view, hybrid warfare is spearheaded by Western governments and reflective of their doctrine. As stated by NATO in November 2021, "To [Russia], hybrid warfare – gibridnaya voina – is something NATO uses against Russia, not vice versa".

This hybrid element–where loosely coordinated or official independent organizations operate–makes the current atmosphere particularly dangerous. Russia appears to aim to thwart attempts to incorporate Ukraine further into the European sphere of influence, both economically and militarily. Historically, Ukraine served as a buffer zone between the powers, such as in 1991, when a newly independent Ukraine became the third largest nuclear power in the world, whose weapons were inherited from the former Soviet Union. So that Ukraine would relinquish its nuclear weapons, the US, the UK, and Russia promised to protect Ukraine's territorial integrity, through the 1994 Budapest Memorandum. That treaty has now been repeatedly violated by the Kremlin, as have subsequent agreements such as the Minsk Protocol aiming for cessation of fighting in eastern Ukraine. While signatories to the Memorandum are not obligated to use military means to enforce the Memorandum, for its part, the US and other nations have not upheld their end of the bargain by defending the territorial integrity of Ukraine, either. The use of non-attributed attacks, such as cyber attacks, or armed proxies helps in perpetuating the Kremlin narrative of appeasement though. Even in the ongoing conflict in Donetsk and Luhansk oblasts, Russia has mainly relied on proxies rather than to commit troops–only when those proxies were on the verge of failing did Russian forces beat back Ukrainian advances. And while it appears Belarus acting as a proxy for Russia is behind the Ukrainian website defacement, unattributed actors conducted a companion destructive attack. Additionally, Recorded Future and others have noted infrastructure associated with APT28, APT29, and NOBELIUM created recently, likely indicates future use. Whether directly controlled or influenced, Russia has demonstrated capability and willingness to conduct extraordinary cyber attacks, as witnessed by the SolarWinds software supply chain attack. Even the use of law enforcement to takedown cyber actors comes into the equation, as the FSB arrests of remnants of the REvil ransomware gang possibly demonstrates attempts to appease the United States and Western nations.

Russia remains a dangerous source of global geo-cyber instability precisely because of its willingness to eschew formal agreements and engage in non-linear warfare—the Kremlin weaponizes confusion and provocation to create a multi-state standoff in eastern Ukraine. Yet Russia also possesses a high tolerance in the cyber realm for collateral damage, as shown by the NotPetya campaign in 2017 and the SolarWinds attack in 2020. With the news of the recent attacks by UNC1151, a group with a likely Belarus-nexus, we can reasonably conclude that Russia is permissive to encouraging other state-sponsored cyber actors to pursue targeting, and furthering its strategic goals.

Conclusions and Recommendations

The Russian military buildup on the Ukrainian border continues to be a risk to regional stability in eastern Europe. A recent article in The Record highlights what a possible Russia invasion might look like, predicting initial information operations before "a series of air- and missile- strikes", amphibious landings at "key cities of Odessa, Kherson, and Mykolaiv", a possible offense from the east and from the southeast rushing "towards the key cities of Dnipro and Zaporizhia". The United States has issued a travel advisory for Ukraine as "Level 4: Do Not Travel" due to COVID-19 and increased threats from Russia. If your organization has personnel in Ukraine, we recommend monitoring ongoing activity through open source intelligence and ensuring up-to-date evacuation procedures and exfiltration in the event of an invasion.

Within the digital space, all organizations should monitor infrastructure against known tactics, techniques, and procedures (TTPs) of Russian state-affiliated actors such as APT28 or NOBELIUM. Russia and its proxies have previously shown little regard for limiting the scope of cyber operations, and may well consider Western European and United States businesses as fair game for disruptive cyber attacks in order to reduce appetite for NATO responses to Russia aggression.

Appendix A: Public resources

FSB arrests of REvil

- https://therecord.media/fsb-raids-revil-ransomware-gang-members/

Biden administration says arrested REvil actor was responsible for Colonial Pipeline

- https://therecord.media/biden-official-one-of-arrested-russian-hackers-carried-out-the-colonial-pipeline-attack/

Microsoft Security technical blog on WhisperGate malware

- https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
  - VirusTotal files for Stage1[.]exe – https://www.virustotal.com/gui/file/a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
  - VirusTotal file for Stage2[.]exe – https://www.virustotal.com/gui/file/dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78

Mandiant reporting on Ghostwriter

- https://www.mandiant.com/resources/ghostwriter-influence-campaign
- https://www.mandiant.com/resources/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity
- https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.