iDEFENSE

Intelligence Alert

Feared Russian Invasion of Ukraine Could Have Global Impacts in Cyberspace

48
Relationships

Severity: High | Threat Type(s): Hacktivism | Cyber Espionage | Cyber Crime

Created on: Jan 7, 2022 7:02 PM GMT
Last activity: Jan 28, 2022 12:26 PM GMT
Last published: Jan 27, 2022 10:52 PM GMT

Summary

The movements of Russian troops and threatening official statements have raised fears that Russia plans to invade Ukraine in the first months of 2022. If a direct military confrontation were to occur, Russia might also undertake cyber-related activity against Ukraine as well as against North Atlantic Treaty Organization (NATO) countries. There could also be impacts on Internet connectivity, such as a cutoff of Russian access to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) payments network or a domestic Internet clampdown under Russia's Internet Sovereignty Law. These potential impacts are described in this report.

Update 16 January 2022: Microsoft has identified destructive malware, disguised as ransomware, on dozens of Ukraine-based government, nonprofit, and information technology organizations. It dubbed this malware Whispergate.

Update 20 January 2022: the US Cybersecurity and Infrastructure Security Agency (CISA), citing the Whispergate campaign, urgently warned senior leaders at "every organization in the United States… regardless of sector or size" of potential Russian threats to essential services and public safety.

Analysis

Key Judgements

- Anyone with business in Ukraine could expect disruptions of essential business and government services, including electricity, transportation, and payments, similar to what happened in the Crashoverride and Petya.A/NotPetya attacks of 2016 to 2017.
- Entities in NATO countries could expect disruptive activity and information operations seeking to erode popular sentiment and political will for supporting Ukraine. Such activity could include state-condoned criminal ransomware or other disruptive attacks against government or critical infrastructure in NATO countries.
- If Western countries follow through on their threats to cut Russia off from the SWIFT financial messaging service, anyone doing business with Russia could expect disruptions in economic activity.
- Organizations in Europe can expect further disruptions to Russian natural gas supplies. Among other tactics, Russian state actors or patriotic cyber criminals could disrupt activities so as to remind Europe of its dependence on Russian gas and thus discourage European countries from harsh measures against Russia.
- Anyone located in or doing business with Russia can expect further crackdown on speech and possibly even the invocation of emergency censorship and restrictions on Internet traffic under the Russian Internet Sovereignty law.

Overview

As 2021 closed, Russia had massed some 100,000 troops on Ukraine's borders. Russian officials and state media made harsh statements claiming that Ukraine's current government poses a threat to Russia and demanding that NATO end its military presence on Russia's borders. Russian Defense Minister Sergey Shoigu even made the outlandish claim that NATO was preparing a chemical-warfare provocation against Russia from Ukrainian territory. In response to these dubious claims, even previous skeptics became increasingly convinced that Russia plans to invade Ukraine in early 2022. Michael Kofman, an expert on the Russian military with generally measured views on Russian intentions, views Russian military action as a realistic possibility.

Military action would have risks and benefits for Russian President Vladimir Putin's government. Analysts generally agree that Russia would have difficulty providing manpower and funds for a sustained occupation of further Ukrainian territory, which would encounter Ukrainian resistance and incur further sanctions from the US and Europe. However, Putin has long sought to restore Russian influence over Ukraine, viewing it as rightful part of Russia.

Some analysts say Putin sees the time for action as now, before Ukraine grows militarily and economically stronger and further strengthens ties with NATO and Western democracies. Indeed, these analysts say, Putin feels himself duty-bound to undo the humiliation Russia endured exactly 30 years ago with the collapse of the Soviet Union in December 1991.

US intelligence agencies assess that Russia has some 100,000 troops already deployed on the border and is prepared to assemble up to 175,000 Russian soldiers for an invasion in early 2022, but that Putin has not decided whether to take that step.

NATO has no obligation to intervene militarily in case of an invasion, as Ukraine is not a member of the alliance, but US officials have reportedly discussed economic sanctions in case of a possible invasion.

Hypothetical dates for a potential attack range from mid-January 2022—after the Russian holiday period encompassing Eastern Orthodox Christmas and "Old New Year's Day," January 7 and 14 respectively—to during or after the Beijing Olympics (a previous Russian invasion of neighboring Georgia took place during the 2008 Beijing Olympics, and Russia's incursion into Ukraine's Crimea region took place just after the 2014 Olympics in Sochi, Russia). A ground assault with tanks would likely have to take place before the spring thaw in March or April that renders roads impassable.

The brinkmanship already forced US President Joe Biden to agree to a phone call with Putin on 30 December 2021, ahead of planned lower-level US-Russian negotiations on 9 to 10 January 2022, Russia-NATO security talks on 12 January 2022, and talks with the Organization for Security and Cooperation in Europe on 13 January 2022. Putin's risk-benefit calculus for a potential invasion would likely depend partly on the outcome of those talks as well as on events in neighboring Kazakhstan, where violent protests led Russia to deploy some 2,500 peacekeeping troops on 6 January 2022 to help the local government restore order.

In the meantime, Russian media and social media proxies continue information operations seeking to blame Ukraine for provoking Russia's military escalation and to undermine support for Ukraine's current government.

President Putin threatened to use unspecified "military-technical" means to repel any "unfriendly steps" by the West; he has implied that the Russian Defense Ministry was formulating various options that Putin might consider.

Analysts fear Putin's government could stage provocations that it could blame on Ukraine or NATO to justify military action, such as by stirring up ethnic or other grievances to provide an excuse for the seizure of Ukrainian territory. Potential types of attack that analysts have hypothesized include a full-scale ground invasion and other measures such as sabotage, air attacks, or long-distance bombardment of Kyiv and other key sites from within Russian territory. Hypothetical scenarios include Russia attempting to occupy coastal areas of Ukraine, to cut that country off from the sea, or to occupy the eastern half of Ukraine. Other hypothetical scenarios envision Russia not attempting to hold territory but rather seeking to topple Ukraine's government or to force it to grant concessions such as abandoning efforts to join NATO. Most scenarios for such a potential attack include a cyber component.

This paper summarizes types of cyber threats that organizations can expect if open military conflict occurs between Russia and Ukraine. Additional analysis of Russian cyber-threat activity appears in reports such as:

- US–Russia Escalation Prospects: Lights-Out Unlikely; Ransomware, Russian Internet Isolation, and Anti-Ukraine Operations Likely
- Biden-Putin Summit May Produce a Lull but Is No Magic Bullet against Russian Cyber-Threat Activity
- Russian Responses to Geopolitical Challenges Include Cyber-Threat Activity against Energy Industry Entities

- Making Sense of Russian Cyber-Threat Activity

Likely Cyber-Threat Activity against Ukraine

Any kinetic offensive would probably also have a cyber component. Anyone with business in Ukraine or other warring parties could expect disruptions of essential business and government services, including electricity, transportation, and payments. As iDefense and other analysts have argued, Russian strategists could use cyber-threat activity to discredit the current Ukrainian government and undermine the population's will to fight.

Judging from past Russian conflicts, this could involve attempts to:

- Cut off telecommunications, as during the Russian takeover of Crimea in 2014.
- Use cyber-enabled information operations and other efforts to foment domestic unrest, as in the so-called "Shatun Plan" that Ukrainian hackers obtained by breaching the systems of Vladislav Surkov, a former Russian top official on Ukraine policy. At least one regional commentator has warned that Russia has "dusted off" the Shatun Plan and is planning renewed war against Zelensky's government.
- Target electric grids and other critical infrastructure and public services, as in the 2015 blackout and the broader Crashoverride operation of 2016 and the Petya.A/NotPetya attack of 2017. Those attacks targeted a wide variety of Ukrainian government agencies providing essential services, and the Petya.A/NotPetya attacks spilled over and caused some US$10 billion in damage to companies worldwide.
- Co-opt Ukrainian communications providers, allowing Russian operatives to reroute traffic through Russian-controlled systems and drop malicious updates; this happened with WNet, the provider whose MEDoc software updates dropped the Petya.A pseudo-ransomware in 2017.
- Demoralize personnel with text messages promising bloody retribution, like the ones Ukrainian soldiers and their families received in 2017 and 2019.
- Distribute a malicious app, such as the malicious version of a popular Ukrainian artillery-targeting app that Russian threat group SNAKEMACKEREL disseminated through online forums and reportedly used to spy on Ukrainian forces.
- Jam and spoof military communications.

Russian Groups

Russian state hackers have participated in these past attacks on Ukraine and on the US and Europe. These groups include SNAKEMACKEREL, SANDFISH, BLACK GHOST KNIFEFISH, WINTERFLOUNDER, and BELUGASTURGEON.

Some Russian cyber criminals have also taken political motives into account in their targeting, in what iDefense has dubbed hybrid ransomware operations and even hybrid distributed denial-of-service (DDoS) operations, as described below.

Disruptive Activity and Information Operations against NATO Countries

NATO countries could expect disruptive activity and information operations seeking to erode popular sentiment and political will for supporting Ukraine. As iDefense has argued elsewhere, Russia's offensive cyber capabilities already have a deterrent effect. In addition, Russian cyber-criminal and state-supported activity has the effect of "degradation," wearing down incident responders and threat intelligence providers through continued activity and false alarms that require repeated mobilization, sowing "discord, confusion, and fatigue" to frustrate defenders of the American electrical grid in a sort of "death by a thousand cuts," as researcher Alex Orleans has suggested.

On 16 December 2021, a joint US cybersecurity advisory reiterated warnings of Russian state-sponsored threats to critical infrastructure. UNC2452 (a.k.a. NOBELIUM), the Russian intelligence-linked group that carried out the Solar Winds supply-chain attack and espionage campaign in 2020, has increased its supply-chain and cloud-focused activity targeting governments and companies. The same could happen to other countries that aid Ukraine.

In addition, non-state actors, such as cyber criminals and state-encouraged hacktivists, can contribute to disruptive activity. iDefense has noted that Russian strategy sometimes resembles throwing spaghetti on the wall; leaders' comments set the tone that encourage ostensibly independent sympathizers, such as cyber-threat actors or Internet trolls, to improvise hostile actions against countries the leaders have attacked. Russian cyber criminals could read Putin's harsh comments in December 2021 as encouragement to target NATO countries. iDefense has argued that ransomware attacks on US critical infrastructure in 2020–2021 align with Russian strategy. Ransomware actors, like the ones who crippled the Kronos payroll system in December, could envision their activities as acts of patriotism.

In particular, Russian threat actors—either state hackers or patriotic cyber criminals—could focus their disruptive activities against energy networks. Russian state-owned energy companies have limited gas supplies sent to Europe in the leadup to winter, reminding it of its dependence on Russian gas. Russian strategists could encourage further ransomware attacks against renewable energy companies, such as a November 2021 incident at Danish wind turbine company Vestas that LockBit ransomware operators later claimed, or continue their information operations against the Green Party in Germany to discourage them from laying sanctions on Russia's Nord Stream 2 pipeline.

SWIFT Cutoff

Discussions of economic sanctions in case of an invasion have included possibly cutting Russia off from the SWIFT international payments system. This idea has surfaced repeatedly in past crises. If Western countries made good on this threat, anyone doing business with Russia could expect disruptions in economic activity. If Russia were to seize and hold additional Ukrainian territory, those areas might also suffer cutoffs in access to SWIFT and other international financial systems.

Over the years, Russian strategists have sought to build a financial infrastructure independent from the Western-dominated global financial system. In case of a SWIFT cutoff, Russian officials have said they could fall back on the Central Bank's System for Transmission of Financial Messages (SPFS) (Russian: Системе передачи финансовых сообщений Банка России or СПФС) for domestic transactions. Media reported in December 2021 that Russia's ally Belarus was also signing up for SPFS. However, limits on SPFS operating hours and message size, and the fact that only 38 banks outside of Russia use it, mean that a SWIFT cutoff would seriously hamper financial communications between Russia and the rest of the world. Russian exporters would need to receive payments from foreign banks through intermediaries in neighboring countries. A more severe sanction would be the freezing of dollar-denominated assets of Russian residents, which could cause panic in the markets for months.

Russian Internet Isolation

Anyone located in or doing business with Russia can expect further crackdown on speech and possibly even the invocation of emergency censorship and restrictions on Internet traffic under the Russian Internet Sovereignty law of 2019. Over the years Russian strategists have sought to establish a sovereign Russian Internet that would be functional even if disconnected from the world Internet. The law's provisions are ostensibly intended to build the infrastructure and procedures to enable centralized control of the Russian Internet during such emergencies. Provisions like the installation of deep packet inspection (DPI) filtering equipment, mapping of routing systems and registration of Internet exchanges, formally enacted on 1 November 2019, have slowly been implemented. Efforts to create a separate Russian domain name system have faced delays. However, if Russian officials were to invoke the law and introduce centralized control and DPI filtering, organizations operating in Russia could experience disruptions in access to the world Internet and the global economic infrastructure. Past efforts to filter out objectionable content and connections, such as an effort to cut off Telegram in 2018 and slow Twitter in 2021, resulted in broader disruptions than intended.

Tensions associated with a potential invasion of Ukraine could lead Russian authorities to intensify their ongoing domestic crackdown on opposition groups and their online presence, as well as on international tech platforms. Human rights groups have faced closure, website shutdowns, or other court action; a famous dissident blogger died in a mysterious fall from a window; heightened Russian intelligence surveillance pressure forced a BBC correspondent to leave Moscow; Russian officials laid an unprecedented fine on Google for refusal to take down prohibited content; and a Russian "localization" law went into effect in 2022, requiring foreign tech platforms to open local offices, thus having local employees subject to law enforcement pressure.

Update 14 January 2022

The Russian talks with the United States (US), the North Atlantic Treaty Organization (NATO), and the Organization for Security and Co-operation in Europe (OSCE) negotiators between 10 and 13 January 2022 did not seem to yield any reduction in tension. On 13 January, US National Security Advisor Jake Sullivan warned that Russia would likely create a provocation as a pretext for an invasion.

In one possible provocation, Russian "peacekeepers" in Transnistria, a breakaway region of Republic of Moldova—were on high alert, ostensibly based on warnings that Ukraine might attempt a provocative attack at a Russian artillery storehouse there. Ostensibly as part of military exercises, the Russian Defense Ministry shipped materiel previously located in eastern Russia westward, raising fears of further military buildup on Ukraine's eastern border.

Several events relating to cyberspace on 14 January added to the sense of uncertainty:

- Ukrainian officials reported that threat actors had breached multiple Ukrainian government websites, posting a threatening message in Ukrainian, Russian, and broken Polish. The message called on Ukrainians to "be afraid and expect the worst," claiming that their personal information had become public. Reports said threat actors had exploited CVE-2021-32648, a vulnerability in the October content management system, a patch for which had been available since September. Ukrainian officials said these kinds of threatening messages are nothing new and claimed their sites had come back online within hours.
    - The image defacing the Ukrainian websites had metadata tying it to Poland, according to Brian Krebs. This, together with the use of the broken Polish language in the note, suggest that this could be an attempted provocation. Russian information operations have long sought to stoke hostility between Ukraine and Poland.
- At the same time, media reported that sensitive military information from Poland was leaked online. The Polish Defense Ministry countered that this leak was due to an employee's error and posed no threat to national security or military functions.

Ransomware Group Raid Adds to Confusion

Also on 14 January 2022, Russia's Federal Security Service announced that it had raided 25 homes of 14 cybercriminals associated with the REvil (Sodinokibi) ransomware. A Moscow court announced the arraignment of Roman Muromskiy and Andrey Bessonov on charges of misappropriation of funds. The choice of these charges may be because Russia's criminal codes provide weak penalties for purely computer crimes, particularly if the victims are not in Russia. The meaning of this arrest, against the background of tensions and fears of cyber conflict, is unclear. The FSB announced that it had carried out the raid "on the basis of an appeal by competent agencies in the US, who informed us about the leader of the criminal group" and his ransomware activities against foreign high-tech companies.

This apparent act of cooperation with the US in fighting cyber crime, at the same time as top officials were making aggressive statements toward the US, could have various explanations:

1) Russia is making concessions on one hand while holding out threats on the other, in an attempt to influence US thinking as US officials prepare further responses to Russia's demands on not letting Ukraine join NATO. Russian officials expected a US written response by the third week of January, according to media reports.

2) Rival law enforcement groups could be either competing with each other or undertaking a good cop-bad cop operation.

3) Russian officials may have ceased to protect the REvil group and instead decided to crack down on it if it began to present more of a liability than an asset for them.

4] The arrest could be a means for Russian intelligence to pressure the REvil actors to cooperate even further with Russian intelligence agencies' espionage or disruptive campaigns.

5] The evidence of the REvil group's lucrative crime spree could serve to underline Russia's hacker prowess and capability of further retaliation in case of harsh US sanctions. In fact, the raid could serve to demonstrate the type of cooperation that Russia could offer or withdraw at will, as a form of leverage over US actions.

6] The timing of the REvil searches came only one day after Ukrainian officials announced the arrest of five members of an unnamed ransomware group, and after Brian Krebs unveiled the identity of wazawaka, who he says is uhodiransomwar, a Lockbit operator. It is unclear whether these various arrests and revelations had any influence on each other.

In any case, although the arrests ostensibly responded to US requests, Russia does not extradite people to the US, and iDefense continues to judge that the seeming move of cooperation with US law enforcement is likely timed to be used as a bargaining chip or threat.

Update 16 January 2022

Ukrainian officials have also been carrying out quiet diplomacy of their own with Russia; President Zelensky has proposed a trilateral meeting between himself, Russian president Vladimir Putin, and US president Joe Biden. In an apparent concession, Ukrainian police have questioned a former leader of the Azov battalion, a Ukrainian nationalist paramilitary group, on Russia's request. Nevertheless, a domestic showdown between President Zelensky and former President Poroshenko highlights an existing weakness in the Zelensky administration that Russian information operations will likely seek to exploit.

Ukrainian security official Serhiy Demedyuk has said the attack that has defaced Ukrainian government websites is attributable to the threat group UNC1151 and is associated with the likely-Russian Ghostwriter campaign that has targeted Eastern European officials. "The defacement of the sites was just a cover for more destructive actions that were taking place behind the scenes and the consequences of which we will feel in the near future," Demedyuk wrote. He has linked UNC1151 to the Belarusian government and has stated the malware the group has used resembles those of the Russian threat group JACKMACKEREL. In 2020, iDefense reported on the Ghostwriter campaign in 2020 and, in 2021, on the campaign against German and Polish officials. Third-party researchers have linked this campaign to the Belarusian military, but Russian operatives are likely to be involved as well. iDefense observes that at least some of the language in Ghostwriter messaging is consistent with a Russia-based author, rather than with a Belarus-based one.

Meanwhile, Microsoft has identified destructive malware disguised as ransomware on dozens of Ukraine-based government, nonprofit, and information technology organizations. Microsoft is tracking the activity as DEV-0586 and has not identified notable associations to other known threat groups. It is also unclear whether this activity has any relationship with the defacements that took place on 14 January.

Police in Sweden are investigating reports of drones flying over nuclear power plants, adding to anxiety about potential attacks on energy systems in Western countries.

Update 18 January 2022

Ukrainian officials consider the defacement campaign, which they call #BleedingBear, and the pseudo-ransomware operation that Microsoft has discovered, dubbed Whispergate, to be part of the same "multi-pronged operation," as US-based cybersecurity journalist Kim Zetter reported. The Whispergate malware has wiped dozens of computers in two Ukrainian government agencies that have also suffered defacements.

Reports have traced the source of the defacement to the October content management system at IT company Kitsoft. Kitsoft has acknowledged that the Whispergate wiper had overwritten its master boot records and that it had shut down its infrastructure in response.

Update 19 January 2022

An analysis of Whispergate by Stairwell provides further detail, including analysis of the stage-3 wiper, based on a sample captured before the Discord server was disabled. It also cites an initial Ukrainian official report suggesting the existence of a Linux variant of the Whispergate malware, in addition to the Windows variants that Microsoft has analyzed.

Update 21 January 2022

Cyber: Researchers reported new findings on the Whispergate/BleedingBear campaign:

- Cisco Talos found that the Whispergate malware had been in Ukrainian government systems since late summer 2021. The wiper, however, was compiled on 10 January 2022.
- ESET researchers said the attackers had used the FUD crypting service, popular among cyber criminals, to obfuscate their code.

Military: Troops from Russia's Far East arrived in Belarus for what Russian media said would be a ten-day military exercise scheduled to start on 10 February. If they were intending to use the alleged exercises as cover for an incursion, this announcement might indicate that Putin's strategists are waiting to see whether their threats and negotiations can win satisfactory concessions before deciding whether to invade. However, planned massive naval exercises, including maneuvers with China and Iran in the Gulf of Oman, have kept the tensions high.

Diplomatic: Meanwhile, US president Joe Biden and French President Emmanual Macron issued confusing statements that suggested differences of opinion on how to respond to further Russian aggression. US Secretary of State Anthony Blinken consulted with European allies and Ukraine and then spoke with his Russian counterpart on 21 January, agreeing merely to continue the dialogue.

One tension-reducing measure that Germany's Economics Minister proposed—to cooperate with Russia on developing renewable energy—appeared intended to help wean Russia from its dependence on fossil fuel revenues. However, Russia continues to resist the transition from fossil fuels.

In other diplomatic initiatives, Putin is seemingly attempting to counter his negative global reputation by playing the role of peacemaker. He has sought to broker the longstanding conflict between Armenia and Turkey and to facilitate the resurrection of the Joint Comprehensive Plan of Action (JCPOA), the agreement under which Iran suspended nuclear weapons development in return for the easing of sanctions. If these initiatives succeeded, Putin could seek to portray himself as a peacemaker and an important voice in world affairs. This is part of the aspiration for dignity that iDefense views as a central motivator of Russian strategy.

Putin may hope that, by wearing his adversaries down with threats and menacing moves, by conducting information operations to erode Western resolve in defending Ukraine, and by portraying himself as a problem-solver in other international conflicts, he will induce Western countries to concede to some of his demands on reducing NATO's presence in Russia's neighborhood.

Update 22 January 2022

Actor Advertises Stolen Ukrainian Government Data, Implies Link with WhisperGate Operation

On the Russian criminal website RaidForums, a newly joined user called "Free Civilian" is advertising "Ukrainian Leaks – 2022: diia.gov.ua – Users 2M." It asks US$15,000 for millions of records of Ukrainian citizens' personal data and promises to sell Ukrainian police, driver, court, and health data later. The ad seems to imply that the data was stolen from the government portal "Diya" during last week's Whispergate/BleedingBear operation. Of this list, only diia.gov[.]ua and judicial websites also appear on lists of websites that the Whispergate campaign compromised. However, other participants in the RaidForums discussion thread as well as Ukrainian cybersecurity analysts doubt the ad is genuine. Ukraine's Digital Ministry announced that many such ads have appeared, likely related to Russia's attempts to undermine confidence in Ukraine's critical infrastructure, and that most of the data being advertised is a hodge-podge of information leaked before 2019. **Note: as of 24 January 2022, the thread had disappeared from RaidForums.**

UK and US Claims of Russian Subversion Efforts and Tie to Energy Targeting

On 20 and 22 January 2022 respectively, the US Treasury Department and the UK Foreign Office claimed that Russia seeks to install a friendly government in Kyiv. The US and the UK issued partially overlapping lists of former Ukrainian politicians who they said have worked with Russian intelligence services to destabilize Ukraine and, in the US Treasury Department's words, "to prepare to take over the government of Ukraine and to control Ukraine's critical infrastructure with an occupying Russian force."

The US Treasury Department sanctioned four people on their list. One of these, Volodymyr Oliynyk, "worked at the direction of the FSB to gather information about Ukrainian critical infrastructure" in 2021, the US Treasury Department wrote, adding that Russia has undertaken "broad cyber operations against critical infrastructure," particularly against Ukraine's energy sector. This implies that Russian intelligence services are using information from Oliynyk in preparing attacks on Ukraine's energy sector. Ukrainian security official Demedyuk said threat actors have intensively probed energy enterprises on the day of the Whispergate/BleedingBear campaign, but also specified that none were breached, suggesting either that the energy entities withstood attempted compromise or that the threat actors saved them for later.

Update 23 January 2022

Military Threat Dims Hope for Diplomatic Solutions

On 23 January, the US State Department, citing an "abundance of caution," announced that it would send home nonessential personnel and employees' family members. It also urged US citizens to consider leaving Ukraine. Ukraine's Defense Ministry assesses Russian troop levels in the region at over 127,000, the CNN has reported. The US government plans to provide Russia with a written response to its demands during the week of January 24, but the prospects for diplomatic solutions appear to have dimmed.

Experts Weigh Prominence of Cyber in Potential Military Confrontation

In a 21 January report, journalist Blake Sobczak asked cybersecurity experts about implications of the WhisperGate pseudo-ransomware campaign. Trellix, a cybersecurity firm merging McAfee Enterprise and FireEye, warned that the threat actors could adapt the malware and use it in a "self-distributing malware attack with global impact," just as the Petya.A/NotPetya campaign has used the EternalBlue exploit for rapid spread. However, Dmitry Alperovitch, former Chief Technology Officer (CTO) at CrowdStrike, said that cyberspace operations "will at best play a very small, supporting function," such as disruptive attacks for psychological effect, and "most of the action will be on the ground in meatspace." Alperovitch has expanded on his scenario for a Russian invasion in a tweet thread

Insurance Coverage

Organizations that may experience Russian disruptive activity stemming from the current conflict should carefully study their cyber insurance contracts. Media reports highlighted a December 2021 New Jersey court ruling that the Ace American cyber insurance company must cover the losses that the Merck company suffered in the 2017 Petya.A/NotPetya attack. The insurance company had resisted paying, saying the attack was an "act of war" and thus was excluded from coverage. However, the court agreed with Merck that, because the insurance policy did not specifically say it would exclude cyber attacks, "Merck had every right to anticipate that the [war] exclusion applied only to traditional forms of warfare."

Updates 24 January 2022

Apparent Hacktivist Attack on Belarus Railways

On 24 January, a Twitter account associated with the Belarus Cyber-Partisans (BCP) announced a hacktivist operation against Belarus Railways. Protesting the buildup of Russian troops in Belarus for a possible invasion of Ukraine, the BCP tweeted, "We encrypted some of BR's servers, databases and workstations to disrupt its operations! Automation and security systems were NOT affected to avoid emergency situations." A supporter posted screenshots purporting to prove they had breached servers at the railway company. The BCP demanded the release of 50 political prisoners and an end to the "presence of Russian troops on the territory of Belarus."

This appears to be a genuine hacktivist operation. Most BCP members are in exile abroad after the 2020 crackdown on protests there. They have continued hacktivist operations included defacement attacks and leaks of sensitive police documents. Further information on this incident, any support it may have received in BCP members' host countries, and its effects will likely emerge in coming days.

Cyber Incident at Canadian Diplomatic Agency

Global Affairs Canada, a government department that manages Canada's diplomatic assets and activity, detected a "cyber incident" on 19 January that caused the agency to limit access to some Internet services, Global News wrote on 24 January. Canada's Communications Security Establishment (CSE) issued a bulletin that evening, warning organizations against "foreign cyber threat activities, including by Russian-backed actors, to target Canadian critical infrastructure network operators, their operational and information technology." CSE did not explicitly attribute the Global Affairs incident to Russia. However, an unnamed "national security source" said suspicions fell on Russia. The source added, "it is not clear if the Russians, the alleged perpetrators, hacked into the system or were able to merely disrupt its service."

Updates 25 January 2022

Preparations for war continued, amid talk of further negotiations. A blackout that paralyzed transportation and other essential services throughout much of Central Asia, though initially attributed to natural causes, underscored the fragility of electrical networks.

US and UK Heighten Decibels on Warnings

- On 23 January, the US Department of Homeland Security sent an Intelligence and Analysis bulletin to state and local governments and critical infrastructure operators. It assessed that "Russia would consider initiating a cyber attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security," according to ABC News, which saw a copy of the document. The DHS acknowledged that it had not yet seen direct cyber threat activity against US critical infrastructure attributable to the Russian government, although it had seen "cyber espionage and potential prepositioning operations in the past." The UK's National Cyber Security Centre (NCSC(has issued a similar warning to organizations to improve their cybersecurity at times of geopolitical tension.

Threats of Tough Sanctions

- Potential US sanctions in case of further Russian incursions into Ukraine include controls on high-tech exports to Russia, Microsoft News (MSN) reported, citing an unnamed "senior official."](https://www.msn.com/en-us/news/world/us-finalizing-plans-to-divert-gas-to-europe-if-russia-cuts-off-supply/ar-AAT7PuJ). "The gradualism of the past is out, and this time we'll start at the top of the escalation ladder and stay there," the official told MSN. A high-tech export ban could deprive ordinary Russians of access to mobile phones and laptops. US officials are negotiating with Middle Eastern and other countries to ensure backup heating fuel supplies to Europe in case of a Russian cutoff, MSN reported.

Saber Rattling

- The US Defense Department ordered some 8,500 troops on alert for potential deployment to Europe, as NATO began a preplanned naval exercise in the Mediterranean. For its part, Russia informed the Irish Air authority it planned a "live fire" air and naval exercise in early February, within 240 Km of the Irish international waters. Though technically legal, such an exercise highlights the vulnerability of Ireland and of nearby international flight paths and undersea cables.

Diplomatic Feelers

- Meanwhile, 25 January headlines in Russian state media agency RIA reported on these developments but also highlighted statements of UK Prime Minister Boris Johnson, French Prime Minister Emmanuel Macron, and other European leaders that diplomatic means could still reduce tension. RIA also reported that Belarus plans to provide emergency energy to Ukraine (hxxps://ria[.]ru/20220125/energiya-1769405460.html). This may be intended as a sign of Belarus' benign intentions, or as a reminder of the vulnerability of Ukrainian networks.

Central Asia Blackout

- In another illustration of the fragility of critical infrastructure, an electricity blackout crippled transportation and other networks in the Central Asian states of Kazakhstan, Kyrgyzstan, and Uzbekistan for several hours on 25 January. Kazakhstan's state power company explained that "the surge in demand for power in the south of country, caused by the failure of the regional power grid, in turn caused another surge on the unconnected 500 kilovolt transmission line joining south and north Kazakhstan, which was completed in 2009." It is true that Kazakhstan had seen increased energy demand after cryptominers moved operations to Kazakhstan from China in recent months, after China cracked down on mining. However, northern Kazakhstan also reportedly receives electricity from Russia, and RIA Novosti reported that the breakdown in Kazakhstan's grid had disrupted this flow.

Updates 26 January 2022

Dubious Promise of No Invasion During Olympics

"We have heard from Russia that it is not their intention to launch any war" during the Beijing Olympics, which run from 4 February to 20 February 2022, Chinese permanent representative to the United Nations Zhang Jun told Russian state media TASS, according to a 25 January Newsweek report. Nevertheless, Russian Foreign Minister Sergey Lavrov claims that Ukraine, egged on by Western powers, is provoking Russia; they may still find a pretext to attack Ukraine during the under the guise of self-defense.

SWIFT Alternatives Remain a Work in Progress

Russian ambassador to China Andrey Denisov told Newsweek that he did not believe the West would cut Russia off from SWIFT. However, just in case Western sanctions did cut Russia off from international financial mechanisms, Russia and China could use Russia's financial information transformation system to settle payments between their two countries. Nevertheless, he acknowledged that this is "a fairly complex issue with numerous elements that requires substantial negotiation work," Russian state news source [RIA Novosti highlighted] http://web.archive.org/web/20220126021135/https://ria.ru/20220125/nato-1769506248.html) that NATO chief Jens Stoltenberg's statements that the alliance is ready to discuss arms control with Russia and will send a response to Russia's proposals this week. However, Stoltenberg has also spoken of bolstering the military presence on NATO's eastern flank, and Russian Foreign Minister Sergey Lavrov dismissed these words, saying Stoltenberg "has lost touch with reality."

Ukraine Reiterates Suspicion of Log4J Link to Whispergate

On 24 January, Yuriy Shchihol, head of Ukraine's Special Communications and Information Protection Service (CIP), summarized the effects of the 13-14 cyberattack on Ukrainian government systems (hxxps://cip.gov[.]ua/ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnikh-organi). He said 22 sites belonging to state agencies had suffered impacts, six of them severe. CIP ordered 70 sites to suspend activity. The disruption lasted three days. Sensitive information was not stolen. He said the investigation is "currently working out the theory of a combination of three attack vectors: a supply chain….and the exploitation of two vulnerabilities—OctoberCMS and Log4j." Initial Ukrainian reports had named the Log4j vulnerability as a possible attack vector, but iDefense has not identified any other evidence or reporting that supports this.

Updates 27 January 2022

Diplomacy and Invasion Speculation

- On 26 January, the US presented Russia its nonpublic **written response** to Russian demands. While not yielding on the main Russian demand for non-expansion of NATO, the US document proposed negotiations on topics such as missile inspections and avoiding clashes in the Black Sea, according to the Wall Street Journal. Kremlin spokesperson Dmitry Peskov said the response gave "little ground for optimism" but also gave room for continued dialogue, according to AP News. Foreign Minister Sergey Lavrov said Putin would consult with top officials and would make a decision soon.

- In contradictory developments, Russia and Ukraine agreed on 26 January, as part of talks under the so-called Normandy Four format with France and Germany, to uphold an ongoing nominal **cease-fire** in eastern Ukraine. All parties agreed to meet in two weeks in Berlin. At the same time, former Russian president Dmitriy Medvedev, now serving as deputy chair of Russia's National Security Council, said in a 27 January interview that direct negotiations between Putin and Ukraine's current leadership were useless, according to RIA news agency (hxxps://ria[.]ru/20220127/ukraina-1769734304.html). RIA's headline implies that Medvedev hopes Ukrainian President Zelensky will soon give way to a more pliable president.

- Amid this flurry of diplomacy, speculations continue on a **possible invasion date**, with arguments centering on muddy roads, Olympics dates, and the state of readiness of amassed Russian troops. A Russian political analyst nicknamed GeneralSVR claimed a date of 18 February in a 26 January posting on Telegram (t[.]me/generalsvr/684). He claimed that Putin had consulted the previous day with military and intelligence leaders, and they had agreed to stage a provocation on that date, followed by missile strikes on Ukrainian infrastructure on the night of 21-22 February. Further, he claimed, Putin would negotiate with Chinese leadership, and would confirm dates within 72 hours. The alleged final decision date, 28 January, coincides with Putin plans to speak with French President Emmanuel Macron. GeneralSVR often has perceptive insights but his possible biases and access to reliable information are unclear. The constantly shifting and conflicting claims about negotiations and invasion plans render all predictions unreliable.

Dubious Claim of WhisperGate Connection with WhiteBlackCrypt Ransomware

On 26 January, Ukraine's CIP agency claimed that elements in the WhisperGate code showed the threat actors attempting a false flag to blame Ukrainians themselves. CIP wrote that the wiper component of the WhisperGate malware—dubbed WhisperKill—" is more than 80% similar to Encrpt3d Ransomware, also known as WhiteBlackCrypt Ransomware" (hxxps://cip.gov[.]ua/ua/news/informaciya-shodo-imovirnoyi-provokaciyi). CIP said the threat actors had chosen this code to pin blame the Ukrainian military, because WhiteBlackCrypt had played a role in previous operations that some had linked with Ukraine. Upon initial code analysis with more precise tools, however, iDefense assesses with a confidence level between 50 and 75% that the Whisperkill sample and WhiteBlackCrypt are actually not the same.

Russian Ransomware Actor Declares "War on the US"

"Wazakawa," the ransomware middleman whom Brian Krebs identified as Mikhail P. Matveev of Siberia, issued three short videos in which he "declared war" on Krebs, on the cybersecurity community, and on the USA. • In the expletive-laden videos, which researcher vx-underground cached on 26 January, an apparently drunk wazawaka slurred, "I declare war on the USA!" • Wazakawa also cursed at cybersecurity researchers in the US, especially at Russians who had found work abroad. He specifically named "Dlma Smilyanets," referring to [Dmitri Smilianets]/#/node/threat_actor/view/58cace56-8d98-4251-aac7-1c66206b1e1c), who served time in a US prison and now works for the cybersecurity firm Recorded Future, and "Khodzhibayev," likely referring to Azim Khodjibaev of Cisco. • He threatened to upload a "CVE," presumably referring to an exploit, that very day, presumably to help other cybercriminals breach his chosen targets.

Meanwhile, Medvedev Lauds Russian-US Cybersecurity Cooperation

In the 27 January interview mentioned above, Dmitry Medvedev also said with pride that the US is "actively requesting cooperation and providing certain information" to pursue cybercriminals, such as credit card fraudsters (hxxps://ria[.]ru/20220127/kiberbezopasnost-1769717008.html). "These are, in essence, joint operations," he said, apparently referring to the takedowns of criminals such as the REvil gang, mentioned above and the arrest of members of the Infraud/UNiCC carding forum. These arrests and Medvedev's statement appear designed to portray Russia as a valuable partner with the power to respond to US requests or to unleash further globally destructive activity.

Additional Updates 27 January 2022

- iDefense analyzed WhisperGate-related files it observed 14 January on two servers within the network of a government insurance bureau in Ukraine. It found a few similarities between the WhisperGate campaign in mid-January 2022 and the NotPetya campaign SANDFISH of June 2017 in being a wiper rather than a financially motivated incident, but that this general overlap is insufficient to draw any further conclusions.

- iDefense has found Dark Web actors posting advertisements for assets that could interest buyers involved in the ongoing Russia-Ukraine conflict. As of 27 January iDefense identified three Dark Web actors advertising databases containing information on Ukrainian and Russian entities as well as advertisements for accesses to networks in Russia and Ukraine, including a bank with administrator access and a power plant. If the accesses are genuine, well-placed adversaries could potentially cripple financial transactions and the energy supply in Ukraine at a wide scale.
- On 27 January the Biden administration released a 100-day "Industrial Control Systems Cybersecurity Initiative -- Water and Wastewater Sector Action Plan " to bolster cybersecurity in water-related critical infrastructure. The plan called for an incident monitoring pilot program, better information sharing, and technical support to water systems. The FBI, the EPA, the NSA, and CISA had issued a warning on 14 October 2021. The CISA alert noted that threat actors, primarily ransomware operators, have breached waste facilities multiple times. In one famous incident, a threat actor breached the water treatment system of Oldsmar, Florida in February 2021 and introduce dangerous levels of lye into the town's drinking water. iDefense analyzed threats to water more broadly in 2020
- In diplomatic developments, both the Chinese and the Turkish governments have warned against rash military action in the Russia-Ukraine conflict. However, both emphasized a need for dialogue to address Russia's "reasonable security concerns," with both Chinese and Turkish leaders reportedly using this identical phrase.

Mitigation

To mitigate the risks of Russian cyber-threat activity and information operations, iDefense suggests that organizations doing business in or with Ukraine, Belarus, Georgia, Kazakhstan, and other countries in Russia's neighborhood, as well as in NATO countries, consider the following:

- Monitoring international news for conflicts that could lead state-linked cyber-threat actors to target those countries.
- Being aware of the possibility that seemingly criminal activity could mask politically motivated activity.
- Maintaining best practices against ransomware such as patching, firewalling infection vectors, updating anti-virus software, enforcing an offsite backup policy, practicing restoration from backups, and using application whitelists.
- Securing remote desktop protocol (RDP) connections with complex passwords, virtual private networks, and network level authentication, if RDP connections must be used.
- Remaining especially alert during the first months of 2022 for tactics, techniques, and procedures (TTPs) associated with Russian threat groups SNAKEMACKEREL, SANDFISH, BLACK GHOST KNIFEFISH, WINTERFLOUNDER, and BELUGASTURGEON; such TTPs could indicate heightened Russian espionage or preparations for disruptive attacks.
- Treating sensationalist media reports skeptically and taking advantage of fact-checking websites such as https://www.bellingcat.com/ and https://www.stopfake.org/en/news/.

Organizations whose business involves Internet or other communications in or with Russia might want to consider the following:

- Maintaining awareness of policy initiatives, cybersecurity campaigns, and cyber-threat alerts issued by the Russian government.
- Considering options for responding to delays in communications traffic and the selective blocking of websites.
- Conducting tabletop exercises to simulate worst-case scenarios such as Russia's self-isolation from the Internet or cutoff from SWIFT. Organizations might consider implementing air-gap of internal banking systems from SWIFT, for example, by having all information on a computer connected to SWIFT be transmitted via flash drive.

iDefense further suggests that organizations consider the mitigations listed in iDefense reporting on threats associated with the following:

- Ransomware
- Supply chains
- Cloud environments
- Cyber-enabled information operations
- Industrial control systems and other operational technologies

Update 16 January 2022: iDefense also suggests that organizations consider

- Searching for the indicators of compromise that Microsoft has identified for the DEV-0586 pseudo-ransomware campaign:
  - a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 (SHA-256 hash of destructive malware stage1.exe)
  - dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 (SHA-256 hash of stage2.exe)
  - cmd.exe /Q /c start c:\stage1.exe 1> \127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 (Microsoft identifies this as "Example Impacket command line showing the execution of the destructive malware. The working directory has varied in observed intrusions.")
- Consulting the recommendations in the 11 January 2022 US Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and National Security Agency (NSA) alert "Understanding and Mitigating Russian StateSponsored Cyber Threats to U.S. Critical Infrastructure. Additional advice on hardening systems against destructive attacks can be found here.

Update 19 January 2022: iDefense also suggests that organizations consider searching for the following indicator of compromise:

- 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d (SHA256 hash of Stage 3 executable (reversed byte-order), build timestamp: 10 Jan 2022 14:39:31 UTC)

Update 20 January 2022: Additional detail on the WhisperGate and indicators of compromise appear in this iDefense report.

Updates 23 January 2022:

- In addition to the CISA alerts mentioned above, on Russian threats to critical infrastructure, iDefense also notes a January 2022 TLP:Green FBI report saying the Fin7 threat group has targeted US entities in the defense and transportation sectors with BadUSB malware. Given the reported links between Fin7 and past disruptive attacks using REvil and DarkSide ransomware families, iDefense suggests that organizations consult iDefense reporting on the BadUSB campaign.
- In light of the court ruling for Merck in its battle to receive insurance coverage for losses from the 2017 Petya.A/NotPetya attack, organizations should carefully study their cyber insurance contracts to make sure they would cover any Russian disruptive activity stemming from the current conflict.

Update 24 January 2022:

- Organizations may consider consulting CISA's list of Known Exploited Vulnerabilities (KEV). CISA added 17 vulnerabilities to the list in the past week and required US civilian agencies to patch 10 of them by the beginning of February 2022. CVE-2021-32648, the October CMS vulnerability that the Whispergate campaign exploited, appears on the list. CISA also named CVE-2021-35247, a SolarWinds vulnerability that threat actors tried to exploit to propagate Log4j attacks to Windows. They failed on this occasion, but threat actors associated with Conti ransomware [have exploited Serv-U vulnerabilities in the past.

Other Properties

Relationships

Mentions

Intelligence Alert

5 of 20

- medium Internet Disruptions in Belarus Amidst Crackdown on Election Protesters
  Date added: **Aug 13, 2020 9:30 PM GMT** Last Published: **Aug 13, 2020 9:30 PM GMT**
- low iDefense Global Research Intelligence Digest for 12 August 2021
  Date added: **Aug 13, 2021 2:56 AM GMT** Last Published: **Aug 13, 2021 2:56 AM GMT**
- low iDefense Global Research Intelligence Digest for July 31, 2020
  Date added: **Jul 31, 2020 10:50 PM GMT** Last Published: **Jul 31, 2020 10:50 PM GMT**
- medium COP26 Climate Talks Convene amid Ongoing Energy-Related Espionage and Information C...
  Date added: **Nov 5, 2021 9:25 PM GMT** Last Published: **Nov 5, 2021 9:25 PM GMT**
- low iDefense Global Research Intelligence Digest for 24 June 2021
  Date added: **Jun 24, 2021 7:41 PM GMT** Last Published: **Jun 24, 2021 7:41 PM GMT**
- high Databases and Network Accesses Potentially Impactful to the Russia-Ukraine Dispute Avail...
  Date added: **Jan 27, 2022 7:07 PM GMT** Last Published: **Jan 27, 2022 7:07 PM GMT**
- low iDefense Global Research Intelligence Digest for 24 January 2022
  Date added: **Jan 24, 2022 11:38 AM GMT** Last Published: **Jan 24, 2022 11:38 AM GMT**
- low iDefense Global Research Intelligence Digest for 20 January 2022
  Date added: **Jan 20, 2022 5:12 PM GMT** Last Published: **Jan 20, 2022 5:12 PM GMT**
- high US Officials Warn of Disruptions as Fear of Russia-Ukraine War Grows
  Date added: **Jan 20, 2022 3:01 AM GMT** Last Published: **Jan 20, 2022 3:01 AM GMT**

Intelligence Report

5 of 8

- Russian Threats to Smart Grid SCADA Devices
  Date added: **Apr 14, 2020 7:56 PM GMT** Last Published: **Apr 14, 2020 7:56 PM GMT**
- Russian Responses to Geopolitical Challenges Include Cyber-Threat Activity against Energy Indus...
  Date added: **Mar 26, 2021 8:09 PM GMT** Last Published: **Mar 26, 2021 8:09 PM GMT**
- Ransomware Roundup from iDefense Analysis
  Date added: **Nov 30, 2021 1:34 AM GMT** Last Published: **Nov 30, 2021 1:34 AM GMT**
- Hybrid DDoS Operations
  Date added: **Sep 2, 2020 6:31 PM GMT** Last Published: **Sep 2, 2020 6:31 PM GMT**
- Hybrid Ransomware Operations
  Date added: **Jun 24, 2020 1:13 PM GMT** Last Published: **Jun 24, 2020 1:13 PM GMT**

Malicious Event 5 of 5

medium Belarusian Chamber of Commerce and Industry Website Defaced by Hacktivists
Date added: **Sep 8, 2020 11:33 AM GMT** Last Published: **Sep 8, 2020 11:33 AM GMT**

high FIN7 Continues BadUSB Device Attacks from August 2021
Date added: **Jan 14, 2022 9:55 PM GMT** Last Published: **Jan 14, 2022 9:55 PM GMT**

low Unknown Actors Message Ukrainian Border Guards With Claims of US Military Intervention
Date added: **Mar 26, 2019 1:00 PM GMT** Last Published: **Mar 26, 2019 1:00 PM GMT**

high Supply-Chain Attack with Unnamed Ransomware Cripples Payroll Provider Kronos, December...
Date added: **Dec 21, 2021 12:54 AM GMT** Last Published: **Dec 21, 2021 12:54 AM GMT**

medium Ukrainian Group Leaks Emails of Top Kremlin Aide
Date added: **Jan 6, 2017 5:10 PM GMT** Last Published: **Jan 6, 2017 5:10 PM GMT**

Country 3 of 3

Canada
Date added: **Aug 21, 2015 12:00 AM GMT** Last Published: **Aug 21, 2015 12:00 AM GMT**

Kazakhstan
Date added: **Aug 3, 2015 3:00 AM GMT** Last Published: **Aug 3, 2015 3:00 AM GMT**

Russian Federation
Date added: **May 6, 2016 3:20 PM GMT** Last Published: **May 6, 2016 3:20 PM GMT**

Target Organization 3 of 3

Public Association Belarusian Railways
Date added: **Oct 16, 2019 4:23 AM GMT** Last Published: **Oct 16, 2019 4:23 AM GMT**

NATO
Date added: **Jan 11, 2017 2:52 PM GMT** Last Published: **Jan 11, 2017 2:52 PM GMT**

Ukranian Ministry Of Defence
Date added: **Nov 26, 2019 2:46 PM GMT** Last Published: **Nov 26, 2019 2:46 PM GMT**

Threat Group 3 of 3

high UNC2452
Date added: **Dec 14, 2020 6:25 AM GMT** Last Published: **Dec 14, 2020 6:25 AM GMT**

extreme SANDFISH
Date added: **Sep 21, 2020 11:05 AM GMT** Last Published: **Sep 21, 2020 11:05 AM GMT**

high SNAKEMACKEREL
Date added: **Jun 6, 2018 1:04 PM GMT** Last Published: **Jun 6, 2018 1:04 PM GMT**

Threat Actor 2 of 2

low wazawaka
Date added: **Apr 4, 2018 5:17 PM GMT** Last Published: **Apr 4, 2018 5:17 PM GMT**

high Ivan Sergeyevich Yermakov (Иван Сергеевич Ермаков)
Date added: **Jul 17, 2018 4:39 PM GMT** Last Published: **Jul 17, 2018 4:39 PM GMT**

Global Event 1 of 1

Russian Internet Sovereignty
Date added: **Aug 17, 2020 2:14 PM GMT** Last Published: **Aug 17, 2020 2:14 PM GMT**

Malware Family 1 of 1

high WhisperGate
Date added: **Jan 25, 2022 4:56 PM GMT** Last Published: **Jan 25, 2022 4:56 PM GMT**

Region 1 of 1

NATO
Date added: **Jul 31, 2015 5:09 PM GMT** Last Published: **Jul 31, 2015 5:09 PM GMT**

Vulnerability 1 of 1

medium CVE-2021-32648 - October CMS Design Error Security Bypass Vulnerability
Date added: **Jan 18, 2022 11:20 PM GMT** Last Published: **Jan 18, 2022 11:20 PM GMT**

Sources

Censor.net	Reputation: **Average**	*Nov 15, 2021*
Допрос ветерана Азова: Немичева вызвали на допрос по запросу Следственного комитета РФ		
http://web.archive.org/web/20220116162945/https://censor.net/ru/news/3310166/harkovskaya_politsiya_vyzvala_na_dopros_veterana_azova_nemicheva_po_trebovaniyu_rf		

Inforesist	Reputation: **Average**	*Jan 23, 2022*
Хакеры продают якобы базы «Дии». Федоров анонсировал запуск услуги защиты		
http://web.archive.org/web/20220123033634/https://inforesist.org/hakery-prodayut-yakoby-bazy-dii-fedorov-anonsiroval-zapusk-uslugi-zashhity/		

Moscow Times	Reputation: **Average**	*Dec 21, 2021*
Putin Warns of 'Military-Technical' Response to Western 'Aggression'		
https://www.themoscowtimes.com/2021/12/21/putin-warns-of-military-technical-response-to-western-aggression-a75891		

Cybersecurity and Information Protection Agency of Ukraine	Reputation: **Average**	*Jan 27, 2022*
hxxps://cip.gov[.]ua/ua/news/informaciya-shodo-imovirnoyi-provokaciyi		

Izvestiya	Reputation: **Below Average**	*Dec 23, 2021*
hxxps://iz[.]ru/1268391/2021-12-23/mchs-rossii-dostavit-185-tonn-gumanitarnoi-pomoshchi-zhiteliam-donbassa МЧС России доставит 185 т гуманитарной помощи жителям Донбасса (The Emergencies MInistry Will Bring 185 Tons of Humanitarian Aid to the Residents of Donbas)		

Stairwell	Reputation: **Average**	*Jan 18, 2022*
Whispers in the noise		
https://stairwell.com/news/whispers-in-the-noise-microsoft-ukraine-whispergate		

Brian Krebs	Reputation: **Average**	*Jan 12, 2022*
https://krebsonsecurity.com/2022/01/who-is-the-network-access-broker-wazawaka/		

Dmitri Alperovitch Twitter	Reputation: **Average**	*Dec 21, 2021*
Tweet		
https://threadreaderapp.com/thread/1473362460673515527.html		

Kim Zetter blog	Reputation: **Average**	*Jan 18, 2022*
Dozens of Computers in Ukraine Wiped with Destructive Malware in Coordinated Attack		
https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped		

New York Times	Reputation: **Average**	*Dec 20, 2021*
U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault		
https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html		

Carnegie Endowment for International Peace	Reputation: **Average**	*Nov 12, 2021*
Ukraine: Putin's Unfinished Business		
https://carnegieendowment.org/2021/11/12/ukraine-putin-s-unfinished-business-pub-85771		

Global Affairs	Reputation: **Average**	*Jan 24, 2022*
Canada suffers 'cyber attack' amid Russia-Ukraine tensions: sources		
https://globalnews.ca/news/8533835/global-affairs-hit-with-significant-multi-day-disruption-to-it-networks-sources/		

CNN	Reputation: **Average**	*Jan 22, 2022*
US Embassy in Kyiv asks State Dept. to authorize departure of nonessential personnel		
https://www.cnn.com/2022/01/21/politics/us-embassy-ukraine-nonessential-personnel/index.html 22		

CSIRT Poland	Reputation: **Average**	*Jan 19, 2022*
http://web.archive.org/web/20220119071908/https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/analiza-cyberataku-na-ukrainskie-zasoby-rzadowe/		

Financial Times	Reputation: **Average**	*Dec 9, 2021*
Why Nord Stream 2 is at heart of US warnings to Putin over Ukraine		
https://www.ft.com/content/650963c2-3e45-4ad0-bc87-0f0b59851a5a		

Radio Free Europe	Reputation: **Average**	*Dec 26, 2021*
Putin To Mull Options If West Doesn't Meet 'Security Guarantees'		
https://www.rferl.org/a/putin-ukraine-security-demands-options/31626828.html		

Moscow Times	Reputation: **Average**	*Dec 29, 2021*
An Annus Horribilis for Russia's Opposition		
https://www.themoscowtimes.com/2021/12/29/an-annus-horribilis-for-russias-opposition-a75871		

Superior Court of New Jersey, Law Division, Union County	Reputation: **Very Reliable**	*Dec 13, 2021*
Merck & Co., Inc. and International Indemnity, Ltd, v Ace American Insurance Company et al		
https://www.documentcloud.org/documents/21183337-merck-v-ace-american		

Belarusian Cyber-Partisans twitter	Reputation: **Average**	*Jan 24, 2022*
https://mobile.twitter.com/cpartisans/status/1485618881557315588?cxt=HHwWlCyrY2g_Z0pAAAA		

Washington Post	Reputation: **Average**	*Sep 15, 2021*
How Belarus's 'Cyber Partisans' exposed secrets of Lukashenko's crackdowns		
https://www.washingtonpost.com/world/europe/belarus-hack-cyber-partisans-lukashenko/2021/09/14/5ad56006-fabd-11eb-911c-524bc8b68f17_story.html		

1 - 20 of 80

accenturesecurity