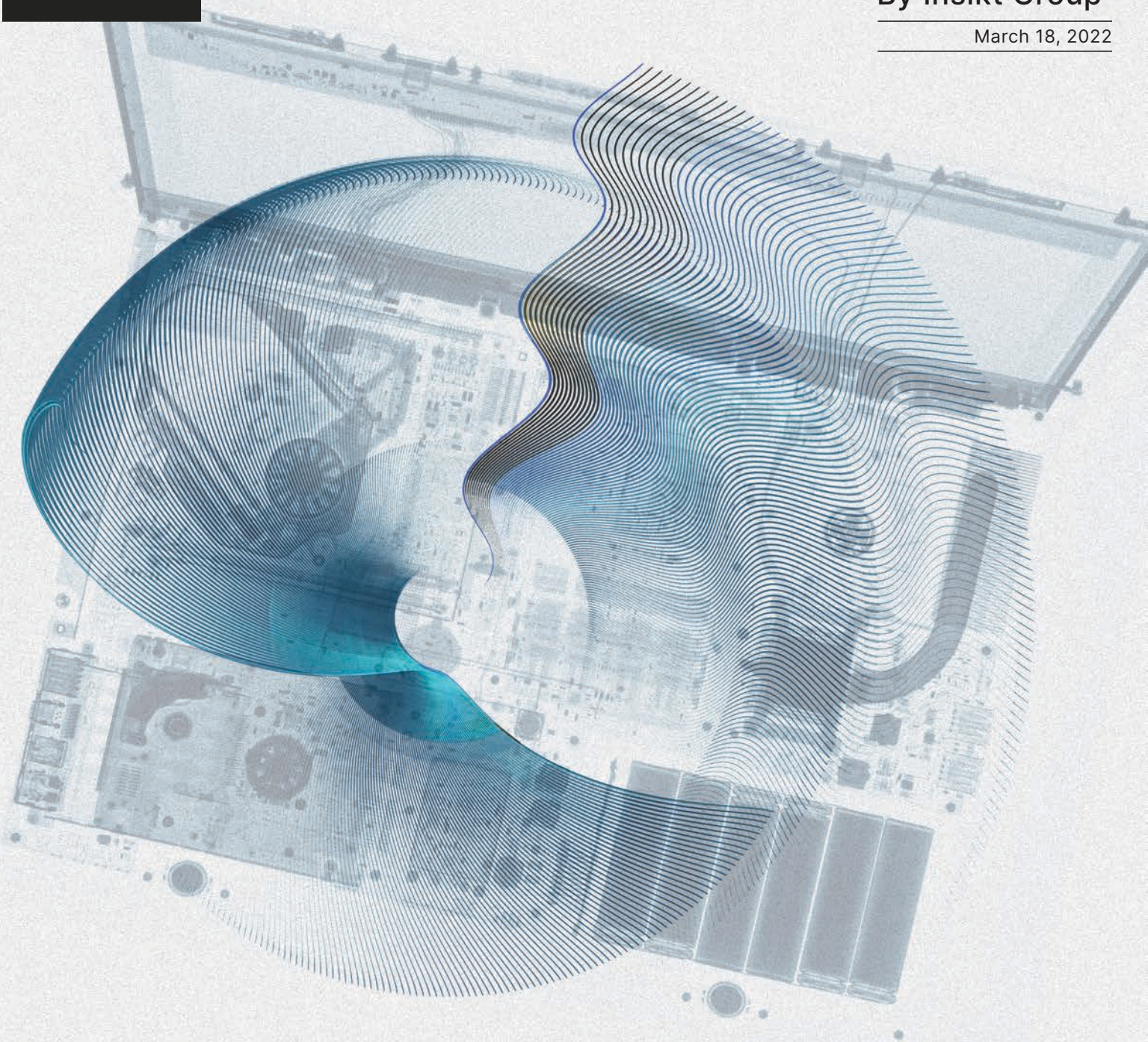
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

March 18, 2022



Ghostwriter in the Shell:

Expanding on Mandiant's Attribution of UNC1151 to Belarus

Recorded Future®

This research expands on Mandiant's public attribution of UNC1151 and Ghostwriter activity to entities in Belarus and describes Russian military organizational influence in Minsk, substantiating a likely nexus to Russian interests. The time frame for our research spans between March 2017 through the present and employs data from the Recorded Future Platform with open source enrichment. It is intended to provide a foundation for understanding the relationship between the threat actor(s) and the broader influences and drivers for activity, as well as augment existing cybersecurity industry reporting and address established knowledge gaps in the understanding of UNC1151 and Ghostwriter activity. This report will be of interest to cybersecurity professionals who track advanced persistent threat actors as well as those seeking greater information on UNC1151 and Ghostwriter.

Executive Summary

On November 16, 2021, Mandiant analysts presented their recent research findings on activity conducted by the cyber threat actor they have designated as UNC1151 and provided insights into the joint cyber and information operations-enabled campaign designated Ghostwriter. The Mandiant team assessed with high confidence that the Belarusian government was responsible for UNC1151 activity that primarily targets European entities and assessed with moderate confidence that the same entity or entities were largely behind the Ghostwriter information operations activity. Nevertheless, Mandiant research did not rule out the possibility of potential Russian government, or other international, involvement in the campaign.

Thus far, there has been a lack of technical evidence indicating Russian involvement, but this is very likely an intended component of the threat activity. We have found many overlaps in tactics, techniques, and procedures (TTPs) used by UNC1151 and Ghostwriter activity and Russian threat activity groups. Additionally, we note that false flags are prevalent among Russian military advanced persistent threat groups, almost certainly due to their training in the Russian military discipline of maskirovka, or deception. Such activity enables Russian military aligned advanced persistent threat (APT) groups to plan and conduct activity in a way that enables plausible deniability. We also emphasize the widespread presence of the Russian military in Belarus, as well as evidence of other Russian high-level influence and training, which all suggest likely Russian involvement and influence in Belarus.

Key Judgments

- Recorded Future does not dispute findings presented by Mandiant in November 2021, which suggest technical links between UNC1151 and Ghostwriter operations and the Belarusian government, likely affiliated with the Belarusian military.
- There is ample evidence to suggest that Russian government entities, specifically entities within the Russian military and academic sector, are likely interacting with the Belarusian government on matters of cybersecurity and information confrontation.
- We have identified reports of high-level meetings between Russian and Belarusian Security Services officials, which indicates that cooperation between the 2 is likely.
- It is likely that Russian military entities, potentially including individuals affiliated with Russian Main Intelligence Directorate (GRU/GU)-related APT groups, operated from, supported, or trained individuals and organizations in Belarus; this assessment is based on long-term Russian Ministry of Defense operations in Belarus.
- The interactions between these entities provide the foundation necessary for Russian state-affiliated military intelligence units to use Belarus as a base of operations or train Belarusian personnel in the disciplines of information warfare and cyber operations.
- The Ghostwriter campaign, along with the UNC1151 activity, was composed of concurrent cyber activity and information operations; GRU/GU APT groups have consistently engaged in operations that leverage multiple aspects of the information domain. These groups highly likely have the capability and intent to conduct aspects of the Ghostwriter campaign and UNC1151 activity.
- Russian GRU/GU APT groups have consistently employed proxies in past operations or engaged in false flag operations to mask their involvement in cyber intrusions; conducting Ghostwriter/UNC1151 activity from Belarusian territory, or involving Belarusian forces in the effort, would likely offer a similar approach to masking Russian involvement.
- The relevance of this research, and the importance of describing the Russian government involvement in Belarusian Ghostwriter and UNC1151 threat activity, is that it reveals how the Russian military can operate from foreign territory or leverage proxies to create challenges to attribution. The synthesis of technical and contextual data, enabled by the Recorded Future platform, can alleviate challenges to attribution.

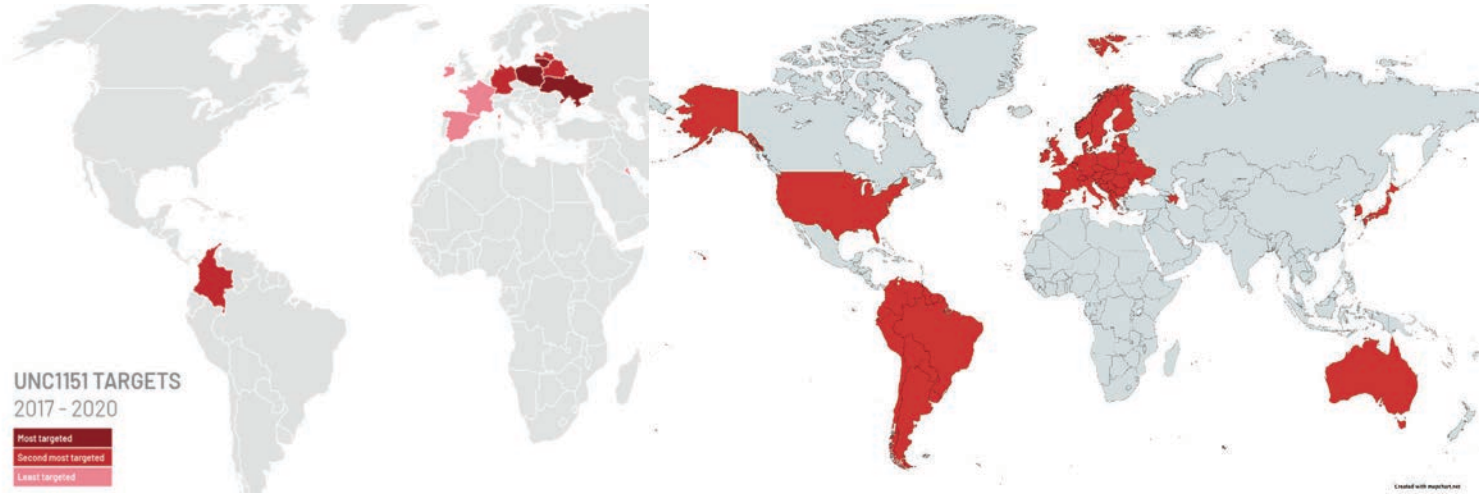


Figure 1: Overview of UNC1151 targets (left) and APT28 and Sandworm targeting (right) (Source: Mandiant, US Department of Justice, Wired, FireEye, Symantec, and others)

Background

Ghostwriter is the designator for an information operations and credential harvesting campaign that has occurred concurrently with likely cyber espionage activity conducted, at least in part, by a threat activity group that FireEye designates UNC1151. According to FireEye, UNC1151 has engaged in infrastructure development, credential harvesting, spearphishing, and targeted intrusions, and Ghostwriter activity largely consisted of social media and website compromise, as well as the development and dissemination of false narratives or forged materials and correspondence to promote divisive narratives. The primary targets for this activity have been NATO-related entities, German politicians, interests in the Baltic region (primarily Latvia and Lithuania), Ukrainian entities, Polish interests, as well as other targets in Colombia, Kuwait, and Ireland. Some of the areas subject to the intrusion and influence activity were also subjected to prior efforts conducted by Russian Main Intelligence Directorate (GRU/GU) groups, as shown in Figure 1.

Initial reporting from Mandiant indicated that narratives promoted as part of the Ghostwriter campaign aligned with Russian security interests. Later reporting identified Russian linguistic artifacts within UNC1151 lure document error messages and described how UNC1151 spearphishing emails were sent from Russian email addresses[1]. In March 2021, a German open source report indicated that spearphishing messages, described as part of the Ghostwriter campaign, were sent to 7 members of the Bundestag (the German federal parliament) and more than 30 members of the state parliament. This report also included statements by the President of the German Federal Office for the Protection of the Constitution (BfV), Thomas Haldenwang, who indicated to the media that German security authorities suspect Russian GRU military intelligence units to be responsible for the activity.

On November 16, 2021, Mandiant researchers released a report and concurrent presentation at CYBERWARCON that assessed "with high confidence that UNC1151 is linked to the Belarusian government" and proposed "with moderate confidence that Belarus is also likely at least partially responsible for the Ghostwriter campaign". According to their research, "Sensitively sourced technical evidence indicates that the operators behind UNC1151 are likely located in Minsk, Belarus … In addition, separate technical evidence supports a link between the operators behind UNC1151 and the Belarusian military". Mandiant researchers maintain that this evidence was either validated by multiple sources or directly observed by their team. Furthermore, Mandiant has asserted that they do not have sufficient evidence to confirm or refute any Russian involvement in this campaign.

Following this attribution, and on January 14, 2022, threat actors likely serving Russian strategic objectives defaced nearly 70 Ukrainian government websites, including websites belonging to the Ukrainian Ministry of Foreign Affairs, Ministry of Defense, the State Emergency Service, Cabinet of Ministers, and Ministry of Education and Science. It later became clear that the defacements were merely cover for the WhisperGate disruptive wiping attack. On January 18, Serhiy Demedyuk, Deputy Secretary of Ukraine's National Security and Defense Council., suggested that the activity may have been conducted by UNC1151 but also noted that the "method of delivery of the malware used in this attack is more characteristic of such groups as Sandworm, APT28, or APT29".

1 It is not clear in the original report, which cites a Polish Radio article, what is meant by "Russian email addresses" in this context. It is unclear if this refers to emails with a known Russian domain/TLD, MX records linked to known Russian email providers, etc. The original Polish Radio report simply states "wysyłane są z rosyjskich adresów e-mail" (sent from Russian email addresses), and can be found archived here: https://web.archive[.]org/web/20220106202135/https://www.polskieradio24.pl/5/3/Artykul/2003195,Uwaga-na-falszywe-wiadomosci-mailowe-Oszusci-podszywaja-sie-pod-Polskie-Radio-SA

Recorded Future does not dispute the technical evidence provided by Mandiant in their November reporting or coincident presentation and agrees that Belarusian infrastructure or resources have likely been employed in the course of this campaign activity. However, we also assess that it is highly unlikely that Ghostwriter activity and UNC1151 operations are solely a Belarusian government effort. Rather, based on contextual evidence as well as overlaps in timing, methods, and operations, it is likely these efforts collectively benefit from Russian government support, training, and direction. The aspect of direction is crucial, given that Russian government policy-makers at the highest levels determine the strategic course of their intelligence operations and any decision for Russian military entities to support, train, or operate from Belarus is likely derived from the upper echelons of the Russian Ministry of Defense.

Threat Analysis

It is unlikely that UNC1151 and Ghostwriter activity is only a Belarusian government endeavor. It is likely that Russian government entities, potentially affiliated with known GRU affiliated Russian APT groups, operated from, trained individuals in, leveraged infrastructure located in, or conducted joint operations with Belarusian entities engaging in Ghostwriter or UNC1151 activity. This assessment takes into consideration the timing and likely capacity for Belarus to solely conduct this activity; the Ghostwriter activity has been ongoing since at least March 2017 but Belarusian cyber operations units were only established in the fall of 2018. Next, because even after the Belarusian cyber operations were established and operational, the teams were likely not large or sophisticated enough to run concurrent information and cyber operations in tandem; Russian military cyber and information warfare operators in the GRU, however, have been engaging in such operations for over a decade and are highly capable in this realm, making it much more likely that either the GRU engaged in the majority of the early UNC1151 and Ghostwriter activity.

It is highly unlikely that the Belarusian domestic IT sector is the source of the cyber operators supporting the UNC1151 and Ghostwriter activity; this assessment is based on linguistic data as well as contextual information showing that many within the domestic IT sector in Belarus have been actively engaging in activity to oppose the Lukashenko regime.

Our analysis consists of 2 main parts. First, we provide context for the relationship between the Russian and Belarusian militaries and information security sectors, which is intended to provide an understanding of how this relationship likely enabled the capabilities, opportunity, and intent observed in the Ghostwriter and UNC1151 threat activity. Second, we provide a comparative analysis between activity conducted by named entities within the existing reporting (Ghostwriter, UNC1151, and Secondary Infektion[2]) and efforts historically conducted by Russian threat groups that engage in information and cyber operations. The goal of this analysis is to provide an understanding of why we believe this activity to have a nexus to known Russian threat activity.

Russian and Belarusian Collaborative Activity

Since at least December 1999, Belarus and Russia have been engaged in an effort to develop a "Union State" alliance between the 2 countries. Such an alliance consists largely of political, military, and economic integration between the 2 nations, while also allowing the Russian government to expand its presence and consolidate its influence in Belarus. The development of the Union State between the 2 countries has led to an increase of Russian military forces and joint exercises, high-level political influence, disinformation, and propaganda in Belarus.

Military Integration

Open source reporting from the Centre for Eastern Studies (OSW), a Polish state analytical center based in Warsaw, notes that the Russian and Belarusian militaries have been close allies since the fall of the Soviet Union. Further, Belarus is a member of the Collective Security Treaty Organization (CSTO), which Russia leads. A separate report indicates that the 2 countries

> *have an integrated air- and missile-defense system, plus a regional group of forces comprised [sic] of four Belarusian brigades and special forces and the Russian 20th Guards Army". Russia leases two military sites: a strategic ballistic missile defense site operated by Russian Aerospace Forces in Hantsavichy [the 474th separate radio engineering center (ORTU)] and the global communications facility for the Russian navy [the 43rd Communications Center of the Russian Navy] in Vileyka.*

2 Secondary Infektion is a suspected Russian information operation active since at least 2014. Broadly speaking, Secondary Infektion tactics, techniques, and procedures (TTPs) rely on forgeries and fake media, principally from false personas, that attempt to enter local sources and penetrate mainstream news. This operation has historically targeted democratic governments and institutions abroad with stories intended to generate rage, confusion, and doubt among domestic audiences in the targeted regions.

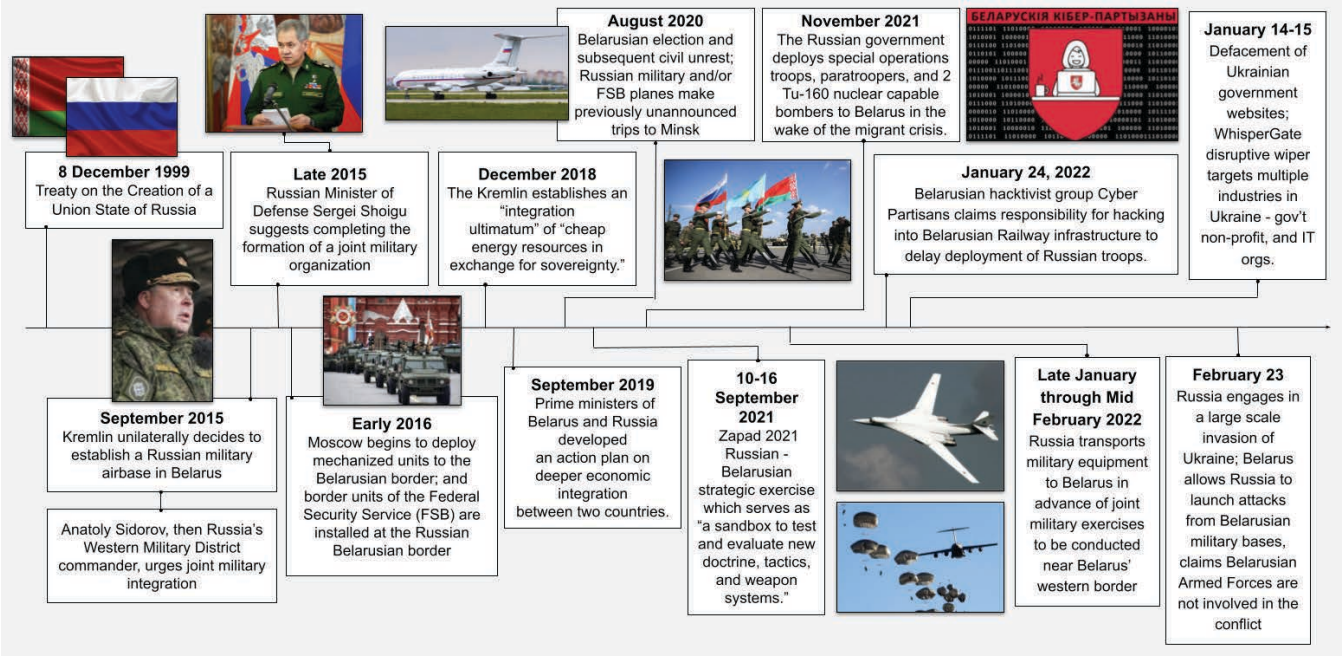


Figure 2: Timeline of Belarus-Russia integration with a focus on Russian military involvement in the region (Sources: FPRI, Bellingcat, USNI, USNews, New York Times, CyberScoop, Tass, and Associated Press)

According to an October 20, 2021, Associated Press report, Russian Defense Minister Sergei Shoigu traveled to Minsk on September 16, 2020, to discuss issues relating to bilateral military cooperation between Belarus and Russia. The following year, Shoigu announced the extension of an agreement on the use of the aforementioned "2 Russian military facilities in Belarus" belonging to the 43rd Communications Center of the Russian Navy and the 474th separate radio engineering center (ORTU). This activity suggests that elements of the Russian military will almost certainly be able to maintain the ability to operate out of Belarus for the near term.

Belarus's Ministry of Defense openly discusses joint cooperation with the Russian armed forces on its official website, noting that such a partnership occurs bilaterally as part of the Russo-Belarusian "Union State" established via the 1999 treaty as well as within a multilateral format via the CSTO and the Commonwealth of Independent States (CIS). Furthermore, this collaboration includes the following:

- Development of the legal and regulatory agreements
- Support of Belarus-Russia Regional Group of Forces
- Air defense cooperation
- Cooperation in arms control agreements
- Training for Belarusian service members at Russian Ministry of Defense military schools
- Joint military-scientific partnerships

Additionally, the Russian military presence in Belarus expanded following the Zapad-2021 military exercises, the subsequent migrant crisis on Belarus's borders, ahead of the February 2022 Allied Resolve exercises, and during a period in which Russia has threatened and subsequently launched a full-scale invasion of Ukraine.

Likely Russian Government High-Level Visits to Belarus

The Russian government likely also dispatched high-level security services personnel to Belarus in mid-August 2020, following the Belarusian presidential election and subsequent protests. Russian security affairs analyst Mark Galeotti stated on August 18 that a Russian special-purpose Tupolev Tu-214VPU (high-altitude command post) aircraft from the Rossiya Special Flight Squadron traveled from Moscow to Minsk and subsequently returned to the Russian capital on August 18 or 19, 2020. The aircraft, bearing tail number RA-64523, is typically reserved for use by the head of the Federal Security Service (FSB), a position currently held by Aleksandr Bortnikov. Although his presence aboard the plane, and in Minsk, could not be independently verified, several media outlets also reported that Bortnikov was believed to be in Belarus.

According to flight records from FlightRadar24, an aircraft bearing the tail number RA-64523 and flight number RSD010 departed Moscow's Vnukovo International Airport (VKO) to Minsk National Airport (MSQ). Early on August 19, the same aircraft, also under flight number RSD010, departed Minsk National Airport for Moscow's Vnukovo Airport, later landing in Moscow. Plane spotting websites have also attributed this airframe, with the same tail number, and what appears to be a long radome on the top of the aircraft, as belonging to the FSB.

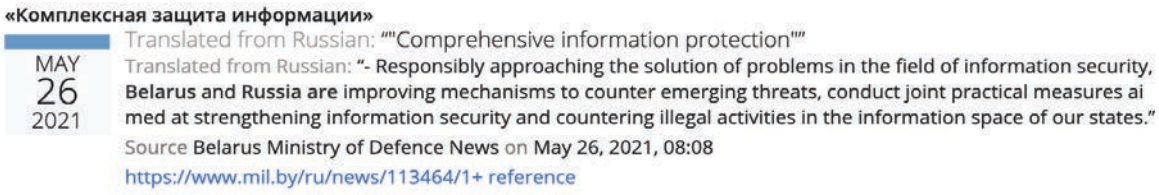


Figure 3: References to joint cooperation in information security (Source: Recorded Future)

A November 17, 2021 article by investigative journalist group Bellingcat on the topic of Russian private military company (PMC) Wagner activity in Belarus confirmed that the Tu-214VPU RA-64523 traveled from Moscow to Minsk. Additionally, Bellingcat indicated that "at least 3 Russian military and/or FSB planes made previously unannounced trips to Minsk in the week following the elections, including 2 flights on 12 August".

This is not the only visit by high-level Russian government officials, as open source reporting indicates that on October 22, 2020, director of the Russian Foreign Intelligence Service (SVR) Sergei Naryshkin traveled to Minsk. According to the report, encrypted chats on Telegram speculated that the purpose of the visit was a meeting between Naryshkin and Belarusian President Alexander Lukashenko. A separate media report indicated that Naryshkin and Lukashenko discussed joint operations, notably how the Russian special services could support Belarus, specifically in matters of common interest. A subsequent meeting between Naryshkin and the Chairman of the State Security Committee of the Republic of Belarus (KGB), Ivan Tertel, was held on June 3, 2021, where the prospect for joint work was again discussed[3], specifically noting that the 2 "agreed to conduct joint work to counter the destructive activities of the West".

Disinformation and Propaganda

In addition to increasing Russian government political and military involvement in Belarus, there was a concurrent increase in disinformation and propaganda, largely supported by Russian state-sponsored media, in the region. Such an effort likely enabled the Russian government to promote narratives likely intended to foster positive sentiments towards Russia amongst segments of the Belarusian domestic population and thus pave the way for a smoother economic, political, and military integration between the 2 states. The use of such influence operations in the region is also indicative of the tenuous relationship between Russia and Belarus, an affiliation that at times could be mutually supportive but also antagonistic. For example, Belarusian leadership and Lukashenko could be amenable to dealing with the Russian government but the Belarusian citizens, who often did not support the Lukashenko regime, were less inclined to support such affiliations.

Research reveals that during the period in which the Russian government applied pressure to Belarus to further integrate their economic, political, and military structures, specifically between 2017 and 2019, "The number of online resources which regularly publish items related to Belarus and contain disinformation, propaganda narratives and hate speech [had] increased". Additionally, "A fully-fledged coordinated network of regional online portals with regular publications containing hate speech against various social, political, religious, and professional groups of the Belarusian population began its activity in 2018". Organizers of the sites promoting such speech frequently promoted the development of a Union State, and some had indirect links to the Russian Embassy in Belarus. A separate research study indicated that around this same period "60% of programming broadcast by TV channels available in Belarus consists of content produced in Russia". The research went on to note that the Belarusian government seldom pushed back against efforts by these outlets to promote false claims, stating that the only instances in which the Belarusian government became involved with fighting false claims were those involving material critical of Belarusian President Alexander Lukashenko.

Around the time of the Belarusian presidential election in August 2020, there were widespread crackdowns on speech, including intermittent internet shutdowns, online censorship, targeting of journalists, as well as credible allegations of widespread torture. At around the same time, Russian journalists from the state-affiliated news outlet RT traveled to Belarus in order to support Belarusian state media. Following the appearance of RT journalists, reports suggested there was a shift in messaging to "propaganda videos slamming protesters as agents of the West". Many of the false narratives or propagandistic claims aligned with Russian state-sponsored narratives.

Cooperation on Information Security, Information Confrontation, and Information Warfare

Since as early as May 26, 2021, Recorded Future has observed open source reporting from official Belarusian government sources indicating joint cooperation in information security between Russia and Belarus.

3 https://web.archive[.]org/web/20210604105140/http://svr.gov[.]ru/smi/2021/06/na-zashchite-interesov-soyuznogo-gosudarstva.htm

On February 26, 2021, Belarus's state-owned news agency Belta cited Alexey Avdonin, a Belarusian analyst with the Belarusian Institute of Strategic Research (BISR), as advocating for Belarus and Russia to engage in a "joint information confrontation" with their opponents. Information confrontation is a Russian military term that describes how to engage in conflict across several domains within the information space that governs, at a minimum, strategic approaches to information operations (IO), cyber activity, psychological operations, and electronic warfare (EW). Such efforts by the Russian military and intelligence/security apparatus are not only conducted in times of open conflict between states, but also occur persistently, targeting both military and non-military targets in an attempt to aid Russian forces in maintaining a favorable position in relation to other nations.

> *Based on the experience of the collapse of the Soviet Union and of Yugoslavia, and on the examples of the colour revolutions in Georgia, Ukraine, Kyrgyzstan, and elsewhere, one can clearly see that major threats do objectively exist and are implemented not only by military means, but primarily by covert and overt methods of political and diplomatic, economic, and information influence, various subversive actions and interference in the internal affairs of other countries. In this regard, Russian security interests require not only to assess these threats but also to determine appropriate measures to respond to them.*

Avdonin further said, "Simultaneous information confrontation is essential because the combined application of force and arms against other states is already an extreme measure. Right now the main goal of our opponents is the control of the consciousness of citizens through various communications channels". He also suggests that NATO is engaging in the effort to control citizens within post-Soviet states by undermining citizens' confidence in the state, discrediting the authorities, and transferring protest sentiment to the streets.

Another report by Rossaprimavera, a pro-Kremlin news outlet, published a report dated February 28, 2020, that carried much of the same material as the February 26 Belta report. The Rossaprimavera report echoed the statement issued by Alexey Avdonin, suggesting that Belarus and Russia engage together on information confrontation efforts against their opponents. Taken together, this activity suggests that Avdonin is resurrecting fears based on Kremlin perceptions, and that these comments are being disseminated to both Belarusian- and Russian-speaking populations in a likely effort to undermine domestic confidence in foreign institutions, delegitimize the protest movement, and normalize the population to the need to engage in information warfare against oppositional forces.

Concerns relating to NATO or "the West" supporting revolutionary sentiments in the post-Soviet territories are an intrinsically Russian issue. Keir Giles' The Handbook of Russian Information Warfare states, "Whether based on a realistic current threat appreciation or not, Russia's perception is that information campaigns in the broadest sense pose a serious and growing threat to the country, implemented and perfected by the United States and the West in the course of a series of regime change operations over decades", noting that these were included among "non-military threats" by then-Chief of General Staff Yuriy Baluyevsky. These threats are enumerated as follows:

In addition to these statements, Recorded Future identified documentation from the 26th Applied Science Conference on Comprehensive Information Defense held from May 25 through May 27, 2021, in Minsk, attended by a number of professionals and delegates from the Russian Federation. One of the attendees, Dr. Vitalii Robertovich Grigorev, is the Head of the Information Confrontation Department at Mirea Russian Technological University, according[4] to the official university website. Additionally, Grigorev was on the committee[5] of the "9th Russian Scientific Conference on Intelligent Systems and Information Confrontation", held in February 2020 and organized by Mirea Russian Technological University.

Grigoriev not only focuses on academic issues and participates in educational conferences but also engages in political and security affairs. Grigoriev was a keynote speaker at the June 21, 2017 Collective Security Treaty Organization (CSTO) meeting on "The role of the CSTO in strengthening collective security in the face of growing threats of hybrid war"; Grigoriev's topic of discussion at the 2017 CSTO meeting was titled "The Role of the Internet's Virtual Social Resources in Real Hybrid Wars". Grigorev is also listed as one of the founders of the "Fund to Support Employees of the Zaslon Special Services and their Family Members". Zaslon was described by one open source article as "a special forces unit for the SVR ([Russian] Foreign Intelligence Service) … [t]rained to operate abroad, in everything from hostage rescue to assassination missions".

4 https://web.archive[.]org/web/20211113091211/https://www.mirea[.]ru/education/the-institutes-and-faculties/institute-for-integrated-security-and-special-instrumentation/the-structure-of-the-institute/department-of-kb-8-information-warfare/

5 https://web.archive[.]org/web/20211211061102/http://analyticswar[.]ru/p%D1%81ommittee/

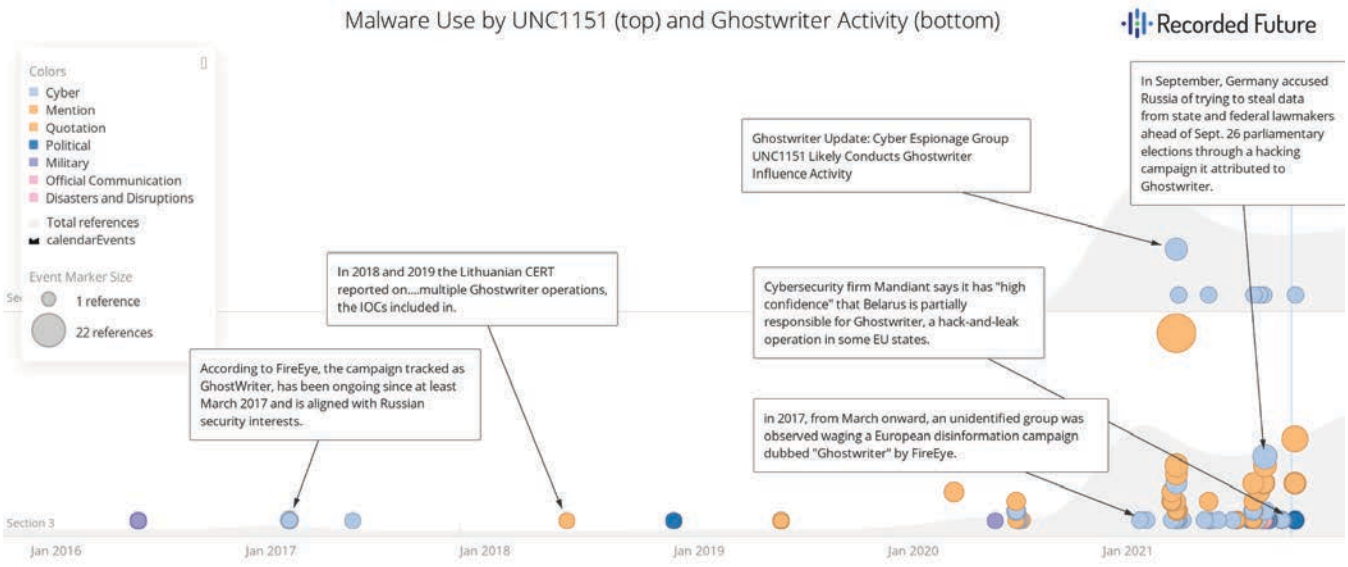


Figure 4: Timeline Revealing UNC1151's malware use as well as overarching Ghostwriter activity (Source: Recorded Future)

UNC1511/Ghostwriter Campaign Activity Versus Historical Russian APT Efforts and Belarusian Interests

Evaluating Mandiant's Findings

Examining Overlaps With Respect to Past Russian Threat Activity

In their most recent report linking UNC1151 and Ghostwriter to the Belarusian government Mandiant maintains that "there have been no overlaps [between the Ghostwriter campaign and UNC1151 activity and] other tracked Russian groups, including APT28, APT29, Turla, Sandworm, and TEMP.Armageddon". In support of this, Mandiant indicates the following points:

- "Sandworm Team has conducted significant credential theft operations during the time UNC1151 has been active, but the techniques used have been distinct. While UNC1151 primarily sent phishes impersonating security notices, Sandworm team has leveraged watering holes designed to redirect users to spoofed login websites.
- "TEMP.Armageddon has conducted extensive targeting of multiple Ukrainian entities during the time UNC1151 has been actively targeting Ukraine. The 2 groups appear to act without knowledge of the other and do not share any malware, infrastructure, or other resources.
- "We continue to assess that Ghostwriter activity is distinct from other information operations campaigns such as Secondary Infektion."
- "Since 2017, UNC1151 operations have leveraged evolving but contiguous TTPs. This evolution is consistent with the maturation of a single organization, and we have not uncovered any evidence of a discontinuity in operators."

Overlaps With Historical Sandworm TTPs

Although Mandiant has indicated that Sandworm and UNC1151 employed different techniques in relation to credential harvesting activity during approximately the same time, there are overlaps in high-level TTPs. Specifically, by looking at historical operations conducted by Sandworm, it is possible to see general similarities between some of the high-level TTPs used by UNC1151. Sandworm has historically leveraged several techniques in relation to spearphishing operations that have been described within the UNC1151/Ghostwriter campaign activity. Additionally, the use of false flag operations in concert with malware campaigns to subvert responsibility may be a feature at play in the UNC1151/Ghostwriter campaign activity.

An October 2020 US Department of Justice indictment against Sandworm operators indicates that the group employed MITRE ATT&CK Subtechnique T1566.001, "Spear Phishing with Malicious Attachments", in their activity targeting credentials for access into 3 energy distribution companies in Ukraine in late spring 2015. This aligns with UNC1151 activity since 2017, in which the threat group employed spearphishing with malicious attachments to harvest credentials from targeted entities. Furthermore, there are tentative indications that suggest UNC1151 may have used spoofed login websites in a credential harvesting operation as Cyjax reported on September 16, 2021, similar to the aforementioned Sandworm activity.

In another technique overlap, and also in the indictment, the Department of Justice describes how later in October 2016, Sandworm targeted Ukraine's State Treasury Service with malware enabled via macros (MITRE ATT&CK Subtechnique T1137.001), a technique also noted in UNC1151's February 2020 likely targeting of the Ministry of Health of Ukraine, according to Mandiant's reporting from April 2021. This technique is employed by a number of groups and not specific to Sandworm. However, it is notable that there are several areas in which we see these overlaps with GRU-related groups like Sandworm and APT28 arise.

In an April 28, 2021 report, FireEye indicated that the following MITRE ATT&CK tactics, techniques, and procedures (TTPs) were affiliated with UNC1151. We have identified several, broad overlaps in these TTPs between and other known GRU related threat activity groups.

- T1547.001: Achieving persistence by adding a program to a startup folder or referencing it with a Registry run key. This is a common tactic as threat activity groups across the spectrum employ this approach for persistence, including APT28, as reported in this December 2020 Trend Micro report.
- T1218.005: Mshta, a utility that executes Microsoft HTML Applications (HTA) files. APT28 employed mshta in the Windows post-exploitation framework and penetration testing tool Koadic in 2018, as indicated in this Palo Alto report.
- T1059.005: Employing Visual Basic Scripting (VBS) for execution. While this technique, like the use of Registry Run Keys, is very common, it is another area in which overlap occurs with several Russian advanced persistent threat groups, including those affiliated with the GRU like Sandworm. Both Dragos and ESET (1, 2, 3) have detailed Sandrworm's use of VBS scripts since at least 2015.
- T1071: Application Layer Protocol. No overlaps have been found with GRU-related threat actors; however, it is notable that Russian APT Dragonfly has employed this technique when targeting the energy and other critical infrastructure sectors, as indicated in this Cybersecurity and Infrastructure Agency (CISA) alert.
- T1105: The transfer of tools from an actor-controlled system to a compromised host, or "Ingress Tool Transfer", is a technique common to many threat activity groups. Notably, however, APT28 has also employed this in their operations, as noted by a July 2021 joint Cyber Security Advisory by the National Security Agency (NSA), CISA, Federal Bureau of Investigation (FBI), and National Cyber Security Center (NCSC). Additionally, according to an October 2020 Department of Justice (DoJ) Indictment Sandworm also remotely installed additional tools on compromised hosts in 2017 when targeting an information technology company.
- T1140: The use of obfuscation and deobfuscation or decoding encrypted files or information in intrusion activity is another technique highly common to many APT groups. We note that, according to a June 2018 Palo Alto report, APT28 used obfuscation techniques in February 2018 to evade detection and Sandworm employed obfuscation in their malware in January 2016 as ESET reported in December 2016.
- T1056: Input Capture. Both APT28 and Sandworm employ the keylogging sub-technique T1056.001 of input capture in their operations. A July 2018 indictment and Trend Micro report notes the APT28 use of this technique and an ESET report describes Sandworm's use of key logging.
- T1059.001: Command and Scripting Interpreter: PowerShell. This tactic is also widely used by many threat activity groups. Inclusive of the GRU affiliated groups using PowerShell commands and scripts for execution are both APT28 and Sandworm. APT28's use of Powershell scripting is called out in the aforementioned December 2020 Trend Micro report as well as the July 2021 joint Cyber Security Advisory. Sandworm's use of Powershell scripting was noted in an October 2018 Dragos' report as well as the previously referenced October 2020 DoJ Indictment against operators from this threat group.
- T1059.007: Command and Scripting Interpreter: JavaScript. No overlaps found with GRU related threat actors however it is notable that Russian APT Turla has employed JavaScript backdoors, as described by a January 2018 report.
- T1559.002: The use of Dynamic Data Exchange (DDE) to execute arbitrary commands has been used by APT28 according to a McAfee November 2017 report as well as the previously discussed June 2018 Palo Alto report.

Finally, Sandworm attempted engage in a false-flag operation during the February 2018 Olympic Destroyer attacks targeting the PyeongChang Winter Olympics Opening Ceremony; at that time, Sandworm attempted to "mimic the malware of other hacking groups-including the Lazarus Group, a state-sponsored hacking team in the Democratic People's Republic of Korea" to divert attention from Russian attribution. Given that this group has employed high-level techniques and tactics such as these, which broadly overlap with UNC1151/Ghostwriter activity, and taking into account that Sandworm is known for conducting false flag operations, it is well within the realm of possibility that the efforts attributed to Belarus may have a nexus to this, or other, Russian APT groups.

Overlaps With Historical APT28 TTPs

In addition to the described high-level overlaps between UNC1151/Ghostwriter campaign activity and historical Sandworm efforts, there are also general associations between this effort and historical APT28 activity, specifically around the targeting of NATO and concurrent information and cyber operations.

According to a June 2021 NATO Strategic Communications Centre of Excellence report, APT28 has targeted NATO since at least 2004. The report suggests an element of timing and media messaging associating Russian interests with the Ghostwriter campaign, stating "The timing of 'Ghostwriter' coincides with the arrival of NATO troops in the Baltics and Poland as part of its Enhanced Forward Presence (eFP). The incoming troops were targeted by intense disinformation campaigns in Russian media and on social media". This activity is similar to historical APT28 activity dating back to at least 2014 when one open source report revealed that the group had "set up a fake website on the Baltic Host logistical planning exercises, which are hosted by one of the three Baltic States — Estonia, Latvia, and Lithuania — and coincided with training programmes carried out by the US Army and NATO forces [in 2014]".

Overlaps With Historical Russian Information Operations TTPs

Recorded Future believes that Secondary Infektion, as well as the Ghostwriter campaign, are 2 aspects of information operations consistent with Russian "active measures"[6], an approach to psychological and narrative warfare developed during the Soviet era that is almost certainly still practiced today by Russian government security service operatives as well as Russian private sector contractors, such as the Internet Research Agency (IRA, or Lakhta Internet Research, LIR).

We believe that Ghostwriter is a closely related, near-parallel information operation to Secondary Infektion, but continue to assess that Secondary Infektion is a broadly defined family of Active Measures campaigns, which include conventional forgeries planted in low-tier sources and forgeries planted through novel intrusion means (such as Ghostwriter). Both what has been observed as Secondary Infektion (non-cyber threat activity, with the exception of the 2019 NHS leaks), and Ghostwriter, each share common themes and content dissemination, most notably in historical campaigns targeting NATO and sensitively sourced intelligence more recently indicating active Secondary Infektion operations against the Belarus/Lithuania migrant crisis. With the exception of intrusion activity, we have observed overlaps in the information operations TTPs of both activity sets in a few cases, namely the use of multiple-use, established personas in a few select examples, as well as passive emulation of real individuals.

According to Mandiant's prior reporting from July 29, 2020, the Ghostwriter campaign had been ongoing since at least March 2017 and "operations have primarily targeted audiences in Lithuania, Latvia, and Poland with narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe, occasionally leveraging other themes such as anti-US and COVID-19-related narratives as part of this broader anti-NATO agenda". Relevantly, Belarus has engaged with NATO on a bilateral basis under the Partnership for Peace (PfP) program since 1995 and as recently as 2018 hosted joint discussions with NATO on regional and international security issues, suggesting it would be unlikely that a Belarusian threat actor would conduct information operations against the organization at this time. However, NATO, and the aforementioned themes inherent in the Ghostwriter campaign, are consistent with longstanding Russian threat activity.

6 Rus: Активное Мероприятие

The Role of the Information Technology and Military Sectors in Belarus

The IT Sector's Role in the Opposition Movement

Within Mandiant's attribution of the UNC1151/Ghostwriter campaign activity to Belarus is the claim that the Belarusian government's cyber capabilities are supported by an experienced pool of professionals domestically. However, the Belarusian domestic information technology sector has publicly spoken out against the actions of the Lukashenko government post-election and has supported opposition efforts. An October 12, 2021 report from the Wilson Center notes that "In the pre-electoral period of June–August 2020, a group of IT professionals developed the online platform Golas (Voice) as an alternative vote counting mechanism". Following the election, on September 8, 2020, the Bell wrote that, "The country's IT sector … has traditionally kept out of politics, but they are now openly supporting the opposition". Additionally, since September 2020, hacktivists calling themselves the Cyber Partisans[7] engaged in website defacements, attacks against Belarusian government resources, and data leaks aimed at exposing abuses by the Belarusian government. The group is reportedly composed of "An army of 30,000 tech-savvy professionals … Coders and software engineers, many of whom are linked to the state-sponsored Hi-Tech Park in Minsk".

Belarusian Military Cyber Operations Program

Mandiant indicated the Belarusian military was likely associated with UNC1151 activity, pointing to the formation of a military IT company in 2018. Insikt Group's research has validated the creation of a unit focused on conducting cybersecurity-related operations in an article titled "В Военной академии формируется рота информационных технологий" or "At a Military Academy a [Military] Company for Information Technologies was Formed" reported by the Belarusian state-owned media outlet Belta. In the article, Defense Minister Andrei Ravkov announced that in November 2018, and within the course of the next conscription effort, a company-level unit would be formed that would focus specifically on information technologies. The article quotes Radkov as stating that information technologies are just a part of a number of scientific-technological developments used in the modern military, and the potential of the Belarusian military is immense, and therefore the goal would be to create a military academy to train these soldiers for these IT units. A follow on report in Belta from February 22, 2019, indicated that 40 people were recruited to serve in the newly formed unit during the autumn of 2018 and that another 20 would be added on in the spring of 2019. According to the article, the military personnel would work with universities as well as other scientific and educational institutions to develop software as well as "special and applied programs". The report also indicated that the training at the academy could be applicable for later employment at the Hi-Tech Park in Minsk but provided no definitive link between the Military Academy and the professional domestic IT sector.

Broader Assessments

A statement by the German Foreign Office in the government provided in a Press Conference from September 6, 2021 in which the government spokesperson indicated that attribution for this activity is as follows:

> *The Federal Government has reliable knowledge on the basis of which the "Ghostwriter" activities can be assigned to cyber actors of the Russian state and specifically to the Russian military intelligence service GRU. The Federal Government regards this unacceptable approach as a threat to the security of the Federal Republic of Germany as well as to the democratic decision-making process and a heavy burden for bilateral relations. The German government urges the Russian government to stop these illegal cyber activities with immediate effect.*

Following this announcement, on November 17, 2021, Dr. Thomas Rid, Professor of Strategic Studies at Johns Hopkins University School of Advanced International Studies indicated that "[The] German gov stands by its assessment, adds: The attribution made by them doesn't rule out other groups having participated as well".

7 Rus: Кибер Партизаны

Outlook

In this research, we have laid out extensive indicators of likely Russian and Belarusian cooperation, including high-level meetings, cyberwarfare training, and public statements. Although we may not have direct visibility into the inner workings of the military intelligence cooperation between the two countries, we have explained the mechanisms that laid the foundation for it as well as the avenues by which it is likely occurring. Additionally, we have detailed the manner in which such cooperation is mutually beneficial, as the activity allows Belarus to improve its technological capabilities in the information warfare space while allowing Russia the ability to escape culpability for its actions.

Therefore, it is likely that if attribution of UNC1151 and Ghostwriter is limited to Belarus, it likely benefits Russian state-sponsored threat activity groups, given that it provides plausible deniability for their operations. Furthermore, such attribution likely emboldens Russian state-sponsored threat activity groups to seek out other similarly hospitable locations to base their operations to provide further challenges to attribution. There have already been indications of Russian information operations moving abroad. A shift in cyber operations to friendly or allied nations could further grant threat actors plausible deniability.

Also, a shift of Russian operational activity to Belarus and the attribution of UNC1151 and Ghostwriter campaign activity solely to Belarus likely risks further alienating Belarus from European allies and threatens any long-term viability of engagement with NATO through the PfP program. Although this may not be the original goal in moving the activity to this location, it appears to be an added benefit for Russian threat actors seeking to drive a wedge between the nations within the Russian sphere of influence and NATO and its allies.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

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