UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests

Blog

Gabriella Roncone, Alden Wahlstrom, Alice Revelli, David Mainor, Sam Riddell, Ben Read, Mandiant Research Team

Nov 16, 2021

12 mins read

Uncategorized Groups (UNC Groups)

Threat Intelligence

Threat Research

Mandiant Threat Intelligence assesses with high confidence that UNC1151 is linked to the Belarusian government. This assessment is based on technical and geopolitical indicators. In April 2021, we released a public report detailing our high-confidence assessment that UNC1151 provides technical support to the Ghostwriter information operations campaign; this assessment, along with observed Ghostwriter narratives consistent with Belarusian government interests, causes us to assess with moderate confidence that Belarus is also likely at least partially responsible for the Ghostwriter campaign. We cannot rule out Russian contributions to either UNC1151 or Ghostwriter. However, at this time, we have not uncovered direct evidence of such contributions.

Cyber Espionage Targeting Most Closely Aligns with Belarusian Government Interests

UNC1151 has targeted a wide variety of governmental and private sector entities, with a focus in Ukraine, Lithuania, Latvia, Poland, and Germany. The targeting also includes Belarusian dissidents, media entities, and journalists. While there are multiple intelligence services that are interested in these countries, the specific targeting scope is most consistent with Belarusian interests. In addition to the targeting scope, UNC1151 operations have focused on obtaining confidential information and no monetization efforts have been uncovered.

- Since at least 2016, UNC1151 has registered credential theft domains that spoof legitimate websites to steal victim credentials. Outside of the major American companies that are used worldwide (Facebook, Google, Twitter), most spoofed organizations have been in the five countries listed above. This has included regional webmail providers, national and local governments, and private businesses.
- Malware based intrusions have also focused on Eastern Europe. Multiple significant intrusions into Ukrainian government entities have been conducted by UNC1151. Though most of the activity was targeting Ukraine, some targeted Lithuania and Poland.
- UNC1151 targeted multiple Belarusian media entities and several members of the political opposition in Belarus in the year before the 2020 Belarusian election. UNC1151 has targeted media entities in Lithuania, Poland, Ukraine, and Latvia, but we have not seen similar targeting of opposition leaders or domestic political activists in these countries. Additionally, in several cases, individuals targeted by UNC1151 before the 2020 Belarusian election were later arrested by the Belarusian government.
- The group has not targeted Russian or Belarusian state entities. It has spear phished intergovernmental organizations dealing with former-Soviet states, but not their governments.

While the majority of UNC1151 operations have targeted countries neighboring Belarus, a small minority have been conducted against governments with no obvious connection to Belarus. There are multiple possible explanations for this targeting, including incidental inclusion on diplomatic mailing lists, or non-public bilateral issues. However, the targeting that does not align directly to Belarusian interests could indicate that UNC1151 also supports additional priorities. These out-of-scope operations mainly took place between 2016 and 2019.

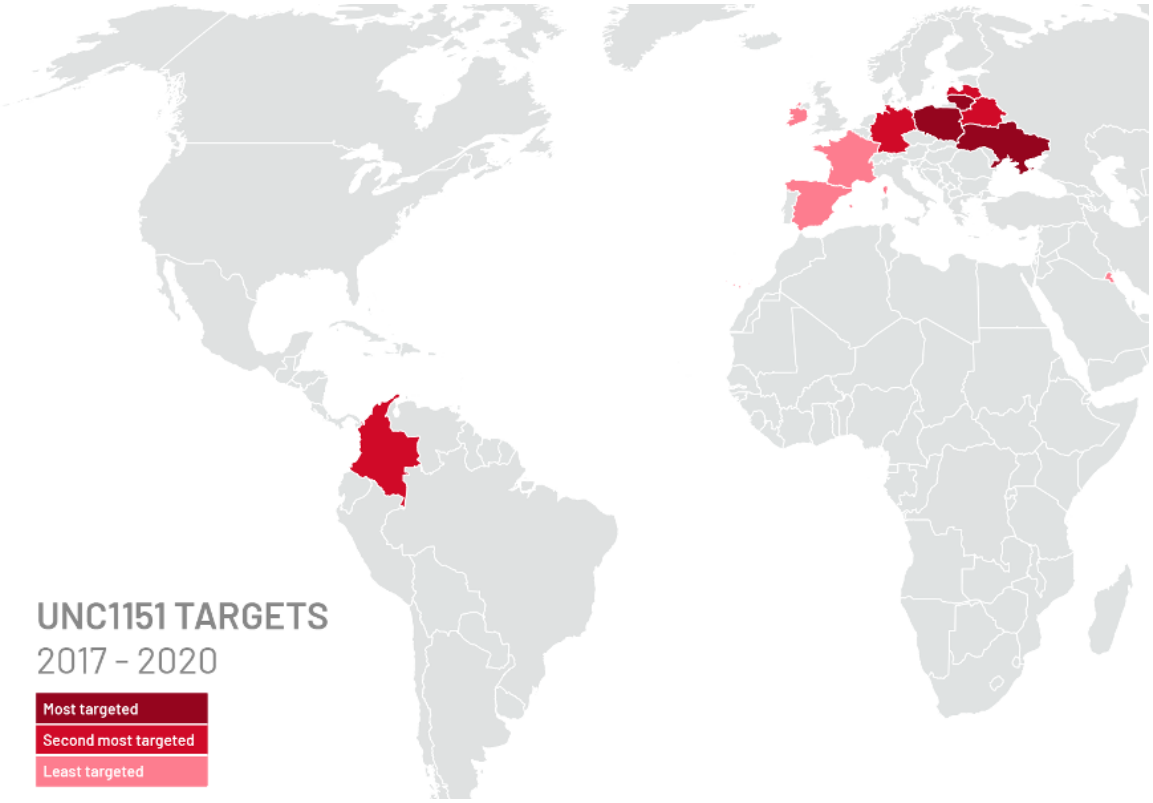

Figure 1: Map of UNC1151 Targeting from 2017 to 2020

- Historical UNC1151 domains have spoofed the websites of entities such as Malta's Government, Kuwaiti Army (mail.kuwaitarmy.gov-kw.ml), France's military, and other targets that are beyond Belarus' immediate geographic neighborhood. More recent UNC1151 domains have spoofed entities related to high priority targets such as Poland, Lithuania, and Ukraine.
- In June 2019, UNC1151 sent a phish with a malicious attachment to 33 recipients. While the majority were in located in Poland, Lithuania, Latvia, and Ukraine, it was also sent to the Colombian, Irish and Swiss governments. In addition, multiple credential theft emails have been sent to the Colombian Ministry of Foreign Affairs.

Technical Evidence Indicates Operators Located in Minsk, Possible Connection to the Belarusian Government.

Sensitively sourced technical evidence indicates that the operators behind UNC1151 are likely located in Minsk, Belarus. This assessment is based on multiple sources that have linked this activity to individuals located in Belarus. In addition, separate technical evidence

supports a link between the operators behind UNC1151 and the Belarusian military.

- Evidence for the location in Belarus and connection to the Belarusian Military has been directly observed by Mandiant.
- These connections have been confirmed with separate sources.

Operational Continuity and No Links to Previously Tracked Groups

Mandiant has tracked UNC1151 since 2017, and during this time there have been no overlaps with other tracked Russian groups, including APT28, APT29, Turla, Sandworm, and TEMP.Armageddon. While we cannot rule out Russian support for or involvement in UNC1151 or Ghostwriter operations, the TTPs used by UNC1151 are unique to this group.

- 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 two 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.

Ghostwriter Operations Aligned with Narrower Belarusian Interests Since Mid-2020

Pre-2020 Ghostwriter information operations were primarily anti-NATO, but since mid-2020 they have focused on Belarus' neighbors.

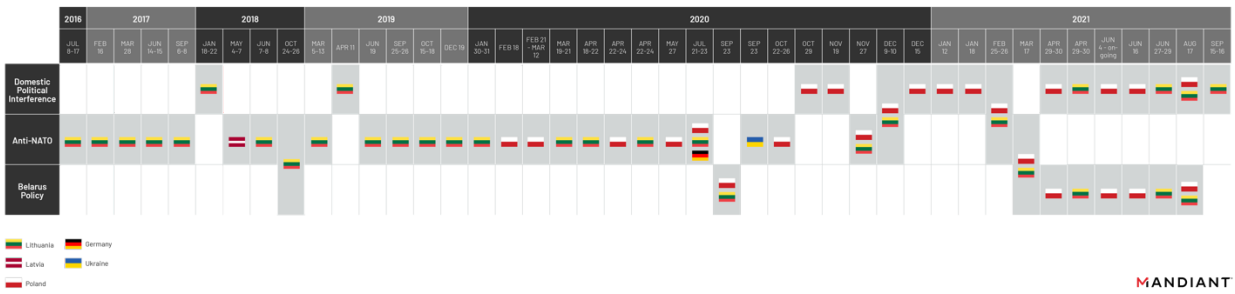

Figure 2: Ghostwriter Operations 2016-2021

From the earliest observed Ghostwriter operation until mid-2020, the Ghostwriter campaign primarily promoted anti-NATO narratives that appeared intended to undercut regional security cooperation in operations targeting Lithuania, Latvia, and Poland. To this end,

observed operations have disseminated disinformation portraying the foreign troop presence in the region as a threat to residents and alleging that the costs of NATO membership are a detriment to local populations. The seeming intended effect of these narratives—to erode regional support for NATO—can serve both Russian and Belarusian interests. We note, however, that the campaign has specifically targeted audiences in countries bordering Belarus, whereas Russia has long promoted anti-NATO narratives both in the region and further afield. Specifically, observed Ghostwriter operations, in this time period and through the present, have almost completely excluded Estonia, which notably does not border Belarus but is a Baltic State, NATO member, and a relevant component of any concerns about NATO's security posture on its eastern flank.

- Twenty-two out of 24 observed Ghostwriter operations conducted prior to mid-2020 promoted narratives that were either directly critical of NATO—including allegations of the deployment of nuclear weapons, NATO troops spreading COVID-19, and crimes committed by NATO troops—or otherwise critical of the presence of foreign troops from allied member states.
- Two additional operations conducted during this period promoted narratives that appeared intended to create controversy in Lithuanian domestic political affairs.

Since the disputed August 2020 elections in Belarus, Ghostwriter operations have been more distinctly aligned with Minsk's interests. Promoted narratives have focused on alleging corruption or scandal within the ruling parties in Lithuania and Poland, attempting to create tensions in Polish-Lithuanian relations, and discrediting the Belarusian opposition. Both governments have strongly condemned the Lukashenka regime's crackdown on demonstrations and extraordinary efforts to stay in power. In addition, several Ghostwriter operations have promoted narratives specific to Belarus, including narratives critical of alleged Polish government support for Belarusian dissidents. It is possible that operations seemingly intended to undermine local confidence in the Lithuanian and Polish governments are a response to what Belarus has claimed to be their intervention in Belarusian domestic affairs. Likewise, operations seemingly intended to create tensions between the two nations may be an attempt to undercut their cooperation, which has in part characterized their responses to Belarus-related issues.

- In August 2020, Ghostwriter personas published articles that portrayed the protests in Belarus as orchestrated by the U.S. and NATO, claiming that NATO is willing to intervene militarily on behalf of the protestors and arguing that the West should refrain from interfering in the "internal affairs" of Belarus.
- Additionally, Ghostwriter operations have promoted narratives that seem designed in part to suggest foreign interference in Belarus, primarily from Poland and Lithuania.
- Since the August 2020 elections, 16 out of 19 Ghostwriter operations promoted narratives defaming the Polish and Lithuanian governments. Of the remaining three narratives, two criticized NATO and one the EU.

- Some operations targeting Poland and Lithuania have promoted narratives with connections to regional disputes involving Belarus. For example, multiple operations have alleged that accidents had occurred at Lithuanian nuclear power facilities. Lithuania has actively opposed the construction and operation of Belarus's Astravyets nuclear power plant, which is located near the Lithuanian border. Likewise, an August 2021 Ghostwriter operation targeting Poland and Lithuania promoted a narrative about a fabricated crime committed by migrants, while Poland and Lithuania were accusing Belarus of orchestrating an outflow of migrants from its borders.
- We have observed some dissemination of these narratives in Russian by what we assess to be campaign assets. The promotion of Ghostwriter narratives in Russian suggests that they are in some way also intended to influence Russian-speaking audiences.

Ghostwriter narratives, particularly those critical of neighboring governments, have been featured on Belarusian state television as fact. We are unable to ascertain whether this is part of a coordinated strategy or if it is simply Belarusian state TV promoting narratives that are consistent with regime interest and being unconcerned with accuracy. Such television programs suggest that some Ghostwriter operations' promoted narratives are particularly relevant to the ongoing internal political conversation in Belarus, and it raises the possibility that discrediting rival governments and Belarusian opposition figures in the eyes of the Belarusian public may be an additional goal of the Ghostwriter campaign.

- We have observed multiple instances of Ghostwriter narratives discrediting the Polish government promoted on Belarusian state-owned TV news. The TV reports have featured allegedly leaked Polish government communications and documents that were promoted in a hack-and-leak style Ghostwriter operation that began in June 2021. They also specifically highlighted narratives that news programs framed as documenting Polish support for the Belarusian opposition. In one instance, a Belarusian TV news report even cited by name a Russian-language Telegram channel that we believe to be a Ghostwriter asset as its source.
- We have additionally observed pro-Belarusian government Telegram channels regularly repost or cite a Russian-language Telegram channel that we have attributed to Ghostwriter.

Uncertainty around Malware Development and Information Operations Content

The sources of written content for Ghostwriter operations and of the malware used by UNC1151 remain uncertain. The creation of content for information operations, especially in multiple languages, requires a distinct skillset from conducting computer intrusions. Likewise, the development of custom malware requires software engineering skills that are distinct from those required to set up a credential theft operation. It is possible that the individuals

supporting these functions are part of the same organization assessed to have a nexus to Belarus; however, the uncertainty and distinct skillsets required for different aspects of this activity creates a possibility for the involvement of additional organizations or countries.

- Ghostwriter information operations have published content in English, Lithuanian, Polish, Latvian, Ukrainian, Russian, and German.
- We have determined that UNC1151 uses GoPhish primarily for their email sending operations – including both cyber espionage and Ghostwriter content dissemination. They often spoof the from envelope of the emails and previously leveraged email delivery services such as SMTP2GO to legitimize themselves. Technical details from early UNC1151 campaigns suggest that the group was unfamiliar with these technologies and may have learned on the job how to use them properly.
- UNC1151 uses credential harvesting domains attempting to spoof legitimate webmail providers, generic login pages, and the legitimate websites of their targets. These credential harvesting domains are sent to victims via phishing email. Over time, UNC1151 domain registration TTPs have shifted. Early domain registration TTPs looked similar to, but did not technically overlap with, clusters of credential harvesting domains we attributed to Russian threat groups. Notably the group has shifted away from using Freenom and towards using Cloudflare services, which may be reflective of increased resources being available to the group.
- UNC1151 has used a proprietary suite of malware, including HIDDENVALUE, and HALFSHELL, and has infrequently been observed using open source or publicly available tools. Though we have observed the use of these early-stage foothold malware families, we have yet to see post-compromise activity.
- UNC1151 has improved in its technical skill since we began tracking the group. UNC1151 malware families are commonly .NET applications with basic command functionality. We have not seen any code overlap between these malware families, though supported commands appear to be similar at a high level. We have observed variants of HIDDENVALUE which support slightly different sets of commands. Prior to HIDDENVALUE, which has been used in several different operations targeting Ukraine and Poland, malware families used by UNC1151 may have been used for limited sets of operations.

Attribution Summary

Mandiant assesses with high confidence that UNC1151 is linked to the Belarusian government and with moderate confidence is linked to the Belarusian military. This is based on the below factors:

- The countries targeted by the majority of UNC1151 operations have strained bilateral relationships with Belarus. While some of these countries are consistent targets of Russian cyber espionage, the specific mix supports a Belarusian nexus.

- Ministries of Defense are the most common government entities targeted by UNC1151, suggesting a military intelligence focus for the group.
- Individual targets, including individuals who are part of the Belarusian opposition and media are of most interest to Belarus.
- Sensitive technical information locates the operation in Minsk, Belarus and links it to the Belarusian Military.
- UNC1151 has conducted operations without a clear, direct link to Belarusian priorities. However, these are a minority of operations and are plausibly explained by multiple factors.

Mandiant assesses with high confidence that Ghostwriter information operations are conducted in support of the Belarusian government and with moderate confidence that they are conducted with Belarusian sponsorship.

- The operations conducted since the disputed Belarusian elections in 2020 have conformed to specific parochial Belarusian government goals and align with the overt actions taken by Belarus against Lithuania and Poland.
- The close technical links between UNC1151 and the Ghostwriter campaign suggest a high likelihood of a shared sponsor.
- However, we lack insight into the generation of the information operations' content.

Mandiant has examined the possibility of Russian participation in UNC1151 and Ghostwriter operations, but we do not have sufficient evidence to confirm or refute a role in these activities. Mandiant has seen high level TTP overlaps with Russian operations and much of the targeting and information operations are consistent with Russian goals. Given the close ties between the governments, collaboration is plausible; however, we have not uncovered direct evidence of Russian government involvement.

- UNC1151's initial focus on NATO's reputation in the Baltics is also a goal of Russia. However, the operations focuses in Lithuania and Latvia, which border Belarus, and were not uncovered in Estonia, which does not.
- Russia has significant offensive cyber and information operations expertise that could have supported the operation.

Outlook and Implications

Belarusian sponsorship of UNC1151 and the links to the Ghostwriter operations showcases the accessibility and deniability of provocative information operations. While the cyber espionage operation was regionally focused and primarily leveraged an open source platform to steal credentials, it was able to support impactful information operations. These types of cyber operations are a one of many tools that governments use to accomplish their goals, and do not exist in a vacuum, but are leveraged alongside other types of operations.