EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization,

Plaintiffs,

v.

John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers,

Defendants.

Civil Action No.

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1

DECLARATION OF NATALIA KRAPIVA IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Natalia Krapiva, declare as follows:

1. I am Senior Tech-Legal Counsel at Access Now, an international non-governmental non-profit organization working to defend and extend the digital rights of people and communities at risk, with particular focus on privacy and data protection, freedom of expression and assembly, digital security, and connectivity.[1] I make this declaration in support of Microsoft's and NGO-ISAC's Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

[1] Available at https://www.accessnow.org/.

2. In my role at Access Now, I serve on the Legal team to shape Access Now's legal advocacy and accountability efforts, including through investigations and strategic litigation. I also work closely with Access Now's Digital Security Helpline,[2] which provides direct technical assistance to "civil society" which are the wide array of individuals, non-governmental and not-for-profit organizations, and community groups that participate in public life, advancing the interests and values of the communities they serve or represent, based on ethical, cultural, political, scientific, religious, philanthropic, or other considerations. For Access Now, members of civil society include journalists, activists, human rights defenders, and other public interest groups and individuals who share the common goals of justice, equality, and human dignity.[3] In that capacity, I often participate in the investigations of phishing, malware, and other digital attacks by closely working with the victims of such attacks and ensuring that the Helpline investigations are informed by sound legal strategy and guidance to maximize effective redress. For example, I have worked on Access Now's investigations of the use of the Pegasus spyware against civil society in Armenia,[4] Serbia,[5] as well as against Russian and Belarusian civil society living in exile in Europe.[6] In particular, I provided legal and risk guidance to the Helpline team, and coordinated with the victims, media, and all the relevant stakeholders on the publications of our findings.

3. At Access Now, I also work on drafting and submitting legal filings in the U.S. and international courts on issues related to spyware, internet shutdowns,[7] encryption,[8] among others. For example, I led the drafting and submission of an amicus brief in the Ninth Circuit Court of

[2] For more information on the Access Now Digital Security Helpline, see https://www.accessnow.org/help.

[3] U.N. Human Rights, Office of the High Commissioner, *Civil Society Resources for NGOs, human rights defenders, and other actors in civic space*, available at https://www.ohchr.org/en/resources/civil-society.

[4] Available at https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

[5] Available at https://www.accessnow.org/spyware-attack-in-serbia/.

[6] Available at https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/; https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

[7] Available at https://www.accessnow.org/press-release/nigeria-twitter-ban-ecowas-court/.

[8] Available at https://www.accessnow.org/press-release/telegram-russia-ecthr-protect-encryption/.

Appeals case, *WhatsApp v. NSO Group*. Similar to this Star Blizzard litigation, the *WhatsApp* case involved members of civil society who were also targeted by threat actors. The amicus brief submitted by Access Now included testimonies from those victims, just as this declaration includes testimonies of members of civil society who were targeted by threat actors.[9] Prior to Access Now, I served as an Assistant District Attorney (ADA) at the Kings County District Attorney's Office in New York. My duties as an ADA included analyzing evidence, drafting legal submissions, making court appearances, and working with victims and witnesses to build cases for criminal prosecution. Prior to that, I held a variety of internships and full-time positions in the United States and internationally with the New York County District Attorney's Office, Queens County District Attorney's Office, New York State Attorney General's Office, the Human Rights Center at the University of California, Berkeley, School of Law, the Office of the United Nations (UN) High Commissioner for Human Rights, and the UN International Criminal Tribunal for the Former Yugoslavia, among others.

4. I obtained my Bachelor's Degree in Political Science from Columbia University in the City of New York and my Juris Doctor degree at the University of California, Berkeley, School of Law. A true and correct copy of the current version of my resume is attached to this declaration as **Exhibit 1**.

5. In my capacity as Senior Tech-Legal Counsel at Access Now, I worked closely with civil society victims in Access Now's investigation into STAR BLIZZARD. My declaration concerns STAR BLIZZARD's impact on civil society.

I. ACCESS NOW AND THE DIGITAL SECURITY HELPLINE

[9] Available at https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/.

6. Access Now is an international non-governmental non-profit organization working to defend and extend the digital rights of people and communities at risk, with particular focus on privacy and data protection, freedom of expression and assembly, digital security, and connectivity.[10] Access Now began as an emergency response team of technologists working to help people get back online and ensure safe communications after the Iranian government blocked internet access and censored content during the 2009 Iranian election.[11] The organization now has a team of more than 100 people across 25 countries, including in the United States and Washington DC. Recognizing that in the 21st century, the threat of digital rights violations compound where they intersect with human rights abuses, Access Now works to hold governments and companies accountable for such violations and abuses in courts around the globe.[12]

7. The Access Now Digital Security Helpline (the Helpline) is a globally distributed team that provides 24/7 incident response and digital security advice to civil society around the world.[13] The Helpline offers real-time, free-of-charge, direct technical assistance and advice to civil society groups and activists, including independent media organizations, journalists, bloggers, activists, and human rights defenders. The Helpline's services are available in English, Arabic, French, German, Italian, Portuguese, Russian, Spanish, and Tagalog. These services include advising civil society individuals and organizations on such issues as threat modeling and risk assessment, secure communications, file storage, web browsing, and social media security, anonymity and censorship, as well as vulnerabilities, phishing, and malware, among others.[14]

[10] Available at https://www.accessnow.org/.

[11] Available at https://time.com/archive/6947035/iran-protests-twitter-the-medium-of-the-movement/.

[12] Available at https://www.accessnow.org/legal-team/.

[13] Available at https://www.accessnow.org/first-digital-security-helpline/.

[14] Available at https://www.accessnow.org/help/helpline-services/.

8. Since it began its work in 2013, the Helpline has responded to over 22,000 digital security requests from civil society in more than 160 countries. The Helpline is a member of CiviCERT, a network of Computer Emergency Response Teams (CERTs), Rapid Response teams, and independent Internet Content and Service Providers that help the civil society prevent and address digital security issues.[15] In 2019, the Helpline also became the first civil society helpdesk to join Forum of Incident Response and Security Teams (FIRST), a network of over 700 incident response and security teams across more than 110 countries, that use their combined knowledge, skills, and experience to promote a safer and more secure global electronic environment.[16]

9. The Helpline's Analyst team focuses specifically on analyzing evidence and investigating digital attacks against civil society, such as spyware, malware, spear phishing, and other attacks. Some of the recently published investigations featuring the Helpline's Analyst team's research includes investigation of NSO Group's sophisticated Pegasus spyware attacks against civil society in Jordan,[17] as well as Russian and Belarusian civil society based in Latvia, Poland, and Lithuania.[18]

II. ACCESS NOW'S INVESTIGATION INTO STAR BLIZZARD

10. In June 2024, Access Now's Helpline received a request from a well-known Russian independent media organization that faces persecution in Russia. At the time, many of the organization's staff were living in exile in countries throughout Europe and the Caucasus, while others remained in Russia. The media organization had received an email from an account that looked like it belonged to a staff member of a partner human rights organization headquartered in

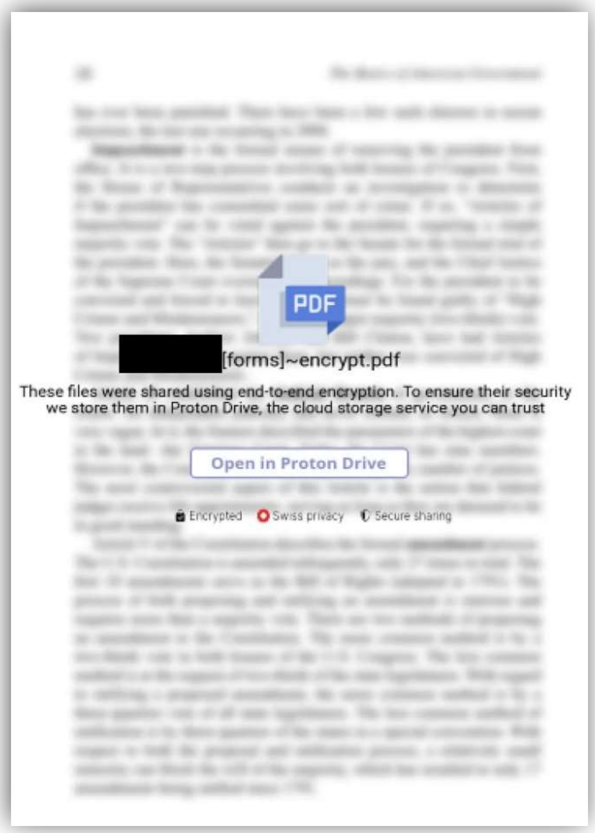
[15] Available at https://www.civicert.org/.

[16] Available at https://www.accessnow.org/first-digital-security-helpline/.

[17] Available at https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/.

[18] Available at https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

Washington DC. The email contained a PDF attachment which appeared to be “encrypted.” In order to “decrypt” the file, the receiver was presented with a “button” to click on that was in fact a URL link embedded within the PDF. One of the independent media’s staff members downloaded the file and tried to open it. Realizing that something was suspicious, the organization contacted the Helpline for assistance. The media organizations' Victim Impact Statement is attached as **Exhibit 2**.



[redacted][forms]~encrypt.pdf

These files were shared using end-to-end encryption. To ensure their security we store them in Proton Drive, the cloud storage service you can trust

FIGURE 1.
Example of STAR BLIZZARD PDF lure. The phishing page is reached by clicking the link. The name of the file is redacted to remove the name of an impersonated organization for privacy and security reasons.

11. The Helpline’s Analyst Team analyzed the suspicious email and discovered that the email account was created on the day of the attack. The Analyst team also analyzed the code in

the URL link that was allegedly required to "decrypt" the PDF file. According to the Analyst team, the code in the link was designed to perform an automatic validation process that, once clicked, would determine certain information about the victim's computer, like the operating system and the system languages, before delivering specific web content. Depending on whether or not the recipient passed the check, they would be redirected either to a page designed to steal their credentials, or a benign page.

12. While the Helpline could not proceed to the next stage to conclusively determine whether or not this attack succeeded, it alerted its peer organization, the Citizen Lab[19] at the Munk School of Global Affairs and Public Policy, University of Toronto (the Citizen Lab) to help further analyze the incident. Subsequently, the Citizen Lab's research determined that the email received by the independent media organization was a highly targeted spear phishing attack (a digital attack that uses carefully tailored information that aligns with a target's personal and professional experiences and activities) by a Russia-based threat group known as STAR BLIZZARD[20] (also known as COLDRIVER,[21] SEABORGIUM, and CALLISTO,[22] among other names).[23] According to the United States and other governments, this group is a subordinate of the Russian Federal Security Service (FSB)'s Center 18.[24]

13. Between June and August 2024, Access Now analyzed five cases of STAR BLIZZARD phishing attacks, with several additional cases analyzed by the Citizen Lab. The

[19] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada. It was founded by Ronald Deibert in 2001. The laboratory studies information controls that impact the openness and security of the Internet and that pose threats to human rights.

[20] Available at https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/.

[21] Available at https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/.

[22] Available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a.

[23] Available at https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/.

[24] Available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a.

details of these investigations are outlined in our respective publications. Access Now's main publication on the investigation is attached to this declaration as **Exhibit 3**.[25] Access Now Helpline's Technical brief is attached to this declaration as **Exhibit 4**.[26] The Citizen Lab's publication outlining their respective investigation is attached to this declaration as **Exhibit 5.**[27]

14. Among the targets identified in the Access Now and Citizen Lab's STAR BLIZZARD investigation are prominent Russian and Belarusian human rights organizations, independent media organizations, as well as former U.S. Ambassador to Ukraine, Steven Pifer. In addition, the hackers behind STAR BLIZZARD also impersonated several DC-based human rights non-governmental organizations (NGOs), as well as another former U.S. Ambassador, to send phishing emails.

15. Since finalizing our publication, Access Now has been investigating several additional phishing cases. Access Now and the Citizen Lab believe that at least one of these additional cases is associated with the STAR BLIZZARD campaign.

16. Access Now also believes that STAR BLIZZARD has likely impacted many more civil society actors from Russia, Belarus, Ukraine, the United States, Western Europe, and beyond. Many organizations and individuals in the civil society space working for human rights in Russia and the region have shared with us that they also received phishing emails that are similar to STAR BLIZZARD or know someone in the community who received such emails. A leading Ukrainian digital security organization and a CiviCERT member, Digital Security Lab (DSL) Ukraine, has shared with us that they have been documenting "waves of targeted phishing attacks using

[25] Also available at https://www.accessnow.org/russian-phishing-campaigns/.

[26] Also available at https://www.accessnow.org/wp-content/uploads/2024/08/Spearphishing-cases-in-Eastern-Europe-2022-2024-technical-brief.pdf.

[27] Also available at https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/.

malicious attachments" against Ukrainian civil society (see the Statement of DSL Ukraine attached as **Exhibit 6).** However, they are not always able to investigate these attacks further due to the lack of resources or inability to gather indicators (see the Statement of DSL Ukraine attached as **Exhibit 6).**

III. THE IMPACT OF STAR BLIZZARD ON SPECIFIC CIVIL SOCIETY ORGANIZATIONS AND INDIVIDUALS

17. STAR BLIZZARD's phishing campaign has inflicted substantial harm on specific individuals and organizations in the United States and internationally.

18. While some targets told us that they did not engage with the phishing emails, others were deceived into clicking on the phishing file or link and entering their user credentials. Even though Access Now did not directly observe credentials being passed back to the attacker's infrastructure, based on the targets' descriptions, it is likely that the attackers leveraged a tool that is specifically designed to capture the entered user credentials and enable unauthorized access. Microsoft documented such techniques used by STAR BLIZZARD in the past.[28]

19. At least one victim reported that after the attack, she lost access to her organization's Google account and one of her contacts received a similar phishing email impersonating her (see Victim Impact Statement attached as **Exhibit 7**). Some victims have also reported highly sensitive records contained in their email accounts leaked on the internet (see Victim Impact Statement attached as **Exhibit 8**). This makes it likely that the STAR BLIZZARD attackers were able to successfully obtain unauthorized access to at least some of the victims' online accounts.

[28] Available at https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/.

20. Most of the targets of STAR BLIZZARD attacks that Access Now and Citizen Lab investigated are Russian NGOs and independent media which defend human rights and democracy, aid refugees, political prisoners, or LGBTQ+ individuals, and report on state corruption, human rights violations, and Russia's illegal war in Ukraine. These organizations have staff located in Russia as well as living in exile around the world, including the United States and Washington DC. One of the targeted organizations in this investigation also works on human rights in Belarus, "Europe's last dictatorship"[29] and Russia's close ally.[30] For these civil society actors, the STAR BLIZZARD attacks are extremely dangerous, since their email accounts contain sensitive information about their staff's identities, activities, relationships, finances, and whereabouts which would likely be of interest to the Russian and Belarusian governments and affiliated actors (see Victim Impact Statements attached as **Exhibits 2, 8, and 9)**.

21. In both Russia and Belarus, these non-governmental organizations and independent media face severe persecution. Some have already experienced criminal prosecution, imprisonment, harassment, intimidation, blocking of their websites, revocation of their legal status, and even physical attacks. Some have been prosecuted under the Russian "fake news" law, which punishes sharing any information about Russia's invasion of Ukraine that contradicts Russian government's position with up to 15 years of imprisonment.[31] Most have received legal designations as "undesirable organizations" and "foreign agents" under the two Russian laws that penalize any cooperation between Russian civil society and Western NGOs and officials and

[29] Available at https://www.economist.com/the-economist-explains/2021/05/25/why-belarus-is-called-europes-last-dictatorship.

[30] Available at https://www.cfr.org/backgrounder/belarus-russia-alliance-axis-autocracy-eastern-europe.

[31] Available at https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/.

which, according to human rights groups,[32] US government,[33] European Union,[34] Organization for Security and Co-operation in Europe (OSCE),[35] and UN experts[36] are repressive tools of retaliation against dissenters. These are repercussions for activities that would be protected under the US First Amendment, such as defending the human right to peaceful protest, supporting political prisoners, or criticizing the war in Ukraine.

22. Due to these threats, the affected organizations and individuals often take multi-layered steps to secure their identities, contact information, and locations, to protect themselves, as well as their staff, partners, clients, and journalistic sources, many of whom are still located in Russia or Belarus. The STAR BLIZZARD phishing campaign was designed to compromise these security measures.

23. One of the targeted individuals in the STAR BLIZZARD attack is Polina Machold, Publisher of Russian independent investigative outlet, Proekt Media. Polina received a STAR BLIZZARD phishing email from an account impersonating a fellow journalist from a U.S. government-funded international media organization (see Victim Impact Statement attached as **Exhibit 9**). Proekt is famous for its high-profile investigations into Russian state corruption, repression, and war crimes in Ukraine, especially involving Russian President Vladimir Putin and his inner circle.[37] These types of investigations require working with sensitive sources and journalists on the ground in Russia who may be in grave danger if their involvement is exposed. Proekt is already a "foreign agent" media that is banned in Russia, with its journalists forced into exile in Europe, United States, and Central Asia (see Victim Impact Statement attached as **Exhibit**

[32] Available at https://www.hrw.org/news/2023/07/25/russia-bill-bans-work-most-foreign-groups.
[33] Available at https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/russia/.
[34] Available at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729297.
[35] Available at https://www.osce.org/files/f/documents/7/5/526720.pdf.
[36] Available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25007.
[37] Available at https://www.proekt.media/en/home/.

9). Proekt was also the first news outlet designated as "undesirable" by the Russian government.[38] Such designation imposes administrative and criminal sanctions on those who collaborates with the organization or even shares their articles on social media.[39] The media's founder, Roman Badanin is known as a personal enemy of Vladimir Putin.[40] According to Polina, Proekt was already "dealing with hacking attempts from Russian State-linked groups," but STAR BLIZZARD "was the most elaborate attempt" to digitally compromise the organization (see Victim Impact Statement attached as **Exhibit 9**).

24. Another independent media organization has also shared with us that the STAR BLIZZARD attack was "the most significant and malicious challenge [they had] ever faced" (see Victim Impact Statement attached as **Exhibit 2**). The attack prompted the media, which was also declared "undesirable" by the Russian government and had four of its staff arrested in the past, to sever working relationships with their staff in Russia and attempt to evacuate some of them (see Victim Impact Statement attached as **Exhibit 2**). According to the organization, they "now live with the distressing knowledge that their [staff's] homes may be raided, and they could face arrest for collaborating with an organization that the Russian government has unjustly labeled as 'undesirable.'" (see Victim Impact Statement attached as **Exhibit 2**).

25. Another STAR BLIZZARD target is a Russian human rights lawyer and the head of a major civil society organization that assists individuals fleeing Russia due to political persecution and their anti-war position (see Victim Impact Statement attached as **Exhibit 10**). For its important work, the Russian government has recently labeled the organization as a "foreign agent." According to the lawyer, while she did not open the STAR BLIZZARD phishing PDF, if

[38] Available at https://rsf.org/en/proekt-first-russian-media-outlet-be-declared-undesirable.
[39] Available at https://ipi.media/russia-must-stop-designating-media-as-undesirable/.
[40] Available at https://www.washingtonpost.com/opinions/2021/09/01/roman-badanin-russia-foreign-agent-law-journalists/.

the attempts to compromise her "had been successful, the potential for harm would have been catastrophic" (see Victim Impact Statement attached as **Exhibit 10**). Such a breach would expose sensitive information about the organization's clients, including their location and the details of their asylum cases, compromising the attorney-client confidentiality and potentially resulting in arrest, imprisonment, "or worse" for these individuals and their families (see Victim Impact Statement attached as **Exhibit 10**). This is especially concerning given that the Russian security services, and FSB in particular, have been reportedly actively engaged in assassinations of asylum seekers and regime critics around the world.[41]

26. For those Russian organizations and individuals who have not been labeled yet as "foreign agents" or "undesirable," there is also an additional risk that Russia can use any contact between them and US and Western-based organizations revealed through their email communications as a pretext for such designations. This could lead to such individuals being criminally charged[42] and imprisoned.[43] For example, another STAR BLIZZARD victim that works with a Russian independent media organization has shared that Russian propaganda channels are urging authorities to imprison their staff and declare the outlet "undesirable" (see Victim Impact Statement attached as **Exhibit 8**). The media organizations' email communications with funders could provide the Russian authorities with the needed pretext for such persecution (see Victim Impact Statement attached as **Exhibit 8**). "Undesirable" designation would especially affect the media's journalists and editors based in Russia, as well as the Russian people across the country who share their opinions and life stories with the media (see Victim Impact Statement attached as

[41] Available at https://www.ft.com/content/46753c29-78f9-485f-8f02-8b203557c40e; https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/.

[42] Available at https://www.hrw.org/news/2017/06/05/russia-rights-activist-facing-charges.

[43] Available at https://www.amnesty.org/en/latest/news/2022/05/russia-activist-mikhail-iosilevich-jailed-for-collaborating-with-so-called-undesirable-organization/.

Exhibit 8). Thus, the unlawful hacking at issue here obstructs the free flow of information and ideas and enables potential follow-on abuses and further violations of fundamental rights. As one media organization put it, "having [their] most sensitive data fall into the hands of [their] worst enemy has left [them] vulnerable and exposed to further oppression" (see Victim Impact Statement attached as **Exhibit 2**).

27. This is why most of the individuals and organizations that Access Now and the Citizen Lab have worked with in the course of the STAR BLIZZARD phishing campaign investigation, requested to stay anonymous and not be mentioned in our public reports. Some individuals were so fearful and emotionally distressed by their information being further exposed to the FSB that they were reluctant to come forward and share any information about the attack even anonymously. Some also experienced shame that they were tricked into interacting with malicious emails and attachments, which may have put their colleagues, clients, and partners at risk.

28. Some STAR BLIZZARD phishing victims have shared with us that they are concerned about the psychological stress caused to their colleagues and clients by the mere realization that the organization was targeted by an FSB-affiliated actor, even if the attack was not successful. The human rights lawyer who was targeted by STAR BLIZZARD shared that her organization works with individuals "who are already under immense pressure due to political threats" they are facing (see Victim Impact Statement attached as **Exhibit 10**). Every new phishing attempt heightens fears that her organization's "efforts to protect human rights and support those fleeing persecution could be undermined" (see Victim Impact Statement attached as **Exhibit 10**).

29. Victims were also concerned that if their community and colleagues learn that they were targeted or impersonated by the STAR BLIZZARD hackers, their reputation and the

reputation of their organization would be severely damaged and people may stop trusting their communications in the future. One of the victims shared with us that a successful STAR BLIZZARD compromise would also "erode the trust" the clients place in her organization, damaging their ability to provide crucial support (see Victim Impact Statement attached as **Exhibit 10**).

30. Indeed, STAR BLIZZARD operations are designed to erode the trust and relationships between civil society organizations and their supporters. In several cases investigated by Access Now and the Citizen Lab, the STAR BLIZZARD emails which targeted Russian and Belarusian civil society organizations impersonated prominent U.S. and especially DC-based organizations. Some of the phishing emails contained the names of these organizations in the malicious PDF files purporting to be human rights reports or other important documents (see **FIGURE 1)**. Such tactics may cause the victims to be reluctant to open emails and attachments from their partner organizations in the future, producing a chilling effect[44] on speech and shrinking civic space.

31. In some cases, the hackers behind STAR BLIZZARD, by using the information they likely obtained from compromising the victim's emails, turned to impersonating the victim to hack their colleagues, partners, and associates. We believe this is what happened to the head of a UK-based organization that helps Russian dissidents and LGBTQ+ individuals, organizes in support of democracy, and raises funds for Ukraine. She received a STAR BLIZZARD phishing email impersonating a prominent DC-based Russian human rights defender and the founder of a US human rights organization that promotes democracy in Russia (see Victim Impact Statement attached as **Exhibit 7**). After the attack, the name of the victim was used in a phishing attack

[44] Available at https://www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect.

against another prominent individual working with civil society, “eroding trust in an already fragile environment” (see Victim Impact Statement attached as **Exhibit 7**).

32. Amongst those affected by the STAR BLIZZARD operations are also former US Ambassadors. For example, as the Citizen Lab revealed, former U.S. Ambassador to Ukraine, Steven Pifer, currently working with the Center for International Security and Cooperation (CISAC) at Stanford University,[45] as well as DC-based Brookings Institution,[46] was targeted with a STAR BLIZZARD phishing email impersonating another fellow Ambassador (see the Citizen Lab’s report attached as **Exhibit 5**). The Citizen Lab stated in their report that they believe that Ambassador Pifer may have been targeted for his extensive networks among sensitive civil society communities, including high-risk individuals from Russia (see the Citizen Lab’s report attached as **Exhibit 5**). Such sophisticated attacks that use social engineering – where a malicious actor poses as someone the victim knows and trusts in order to deceive them and obtain unauthorized access to their computer systems[47] – undermine professional and personal relationships and damage confidence and trust between people.

33. Finally, in addition to putting individuals’ and organizations’ safety, relationships, and reputation at risk, the STAR BLIZZARD attacks have also significantly disrupted the ability of the civil society affected by the phishing campaign to do their important human rights work. One victim shared that because her Gmail account was locked for three days after the phishing attack, her organization was “severely hindered in [its] ability to assist another NGO with their grant application for the evacuation of LGBTQA+ individuals persecuted in Russia” (see Victim Impact Statement attached as **Exhibit 7**). The organization also lost access to their calendar and

[45] Available at https://cisac.fsi.stanford.edu/.
[46] Available at https://www.brookings.edu/.
[47] Available at https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

missed other critical communications, significantly setting back their operations (see Victim Impact Statement attached as **Exhibit 7**). In the aftermath of the phishing attack, the affected organization also had to undertake a comprehensive review of their digital and personal security, which took over two weeks and required costly resources from an organization that has no paid staff, adding "an enormous workload [and] straining the mental and physical health of [their] activists, who are already working tirelessly" (see Victim Impact Statement attached as **Exhibit 7**).

34. Another organization shared that following the attack, "[t]he financial and administrative burden of evacuating [their] team members who agreed to leave Russia [had] been immense" (see Victim Impact Statement attached as **Exhibit 2**). The STAR BLIZZARD operation has left the organization's entire team "distressed and unable to work effectively for an extended period following the attack" (see Victim Impact Statement attached as **Exhibit 2**).

IV. THE IMPACT OF STAR BLIZZARD ON CIVIL SOCIETY AS A WHOLE

35. Beyond the specific individuals and organizations targeted or impersonated in this phishing campaign, the STAR BLIZZARD has a profound effect on civil society, the civic space, and the security of journalists and human rights defenders as a whole.

36. The hackers behind the STAR BLIZZARD campaign use sophisticated techniques that carefully study the individuals and organizations, their work, their contacts and relationships, and other surrounding context, and exploit it to steal credentials and conduct espionage on behalf of the Russian regime. These tactics instill fear and reluctance in the civil society to communicate and participate in civic spaces.

37. All individuals, and especially journalists and activists who often live in exile or are operating in extremely repressive environments, rely on the internet and online

communications for exercising their fundamental rights, the same rights protected by the U.S. Constitution and affirmed in international law. Weaponizing online email platforms to steal credentials and conduct espionage violates not only the fundamental right to privacy, but also rights to receive and impart information, organize, and peacefully assemble for civic and political action, online and off. Hacking and surveillance of journalists and independent media also violates press freedom, explicitly protected under the U.S. First Amendment.

38. STAR BLIZZARD also undermines the trust in digital security among civil society. In their recommendations, digital security organizations often advise not to interact with strangers and avoid "suspicious" emails, links, or attachments. However, the malicious emails and attachments in the STAR BLIZZARD phishing campaign were not immediately "suspicious," but, on the contrary, looked like they were coming from a trusted source. Since STAR BLIZZARD hackers are so effective at impersonating the individuals and organizations known to the victim, it could be very difficult to immediately realize you are communicating with a malicious actor.

39. In some ways, sewing confusion and self-doubt is the goal. Thus, the STAR BLIZZARD attacks instill in the victims and others in the community a sense that no matter how closely they follow digital security recommendations, it will not be enough to make them feel secure. This leaves them feeling like in order to achieve security, they would need to stop communicating altogether or otherwise not bother following digital security protocols. This deters civil society actors from communicating and associating online, resulting in a chilling effect, and also discourages them from taking digital security measures.

V. <u>COURT MUST TAKE ACTION TO ADDRESS THE HARMS OF STAR BLIZZARD</u>

40. Since we published our investigation, more civil society individuals are contacting Access Now with suspected phishing cases. We believe that at least some of them were targeted by STAR BLIZZARD. This leads us to think that the attacker is still active and not deterred despite governments, companies, and civil society exposing their malicious activities.

41. Thus, we are asking the court to take urgent action to prohibit the threat actors behind STAR BLIZZARD from continuing to engage in the harmful and illegal behavior that targets civil society organizations and their partners in the United States and internationally. Stepping in and preventing STAR BLIZZARD from relying on U.S. internet infrastructure, such as domain registries/registrars and IP address hosting providers, will help protect vulnerable civil society and independent media organizations from being victimized, and the respectable U.S. NGOs and individuals, like Ambassador Pifer, from having their good name and reputation exploited for espionage and other harmful activities.

42. In addition, by allowing the discovery in this case and subpoenaing the domain registrars or hosting providers used by STAR BLIZZARD, the court has an opportunity to reveal the information about the attackers that could enable further enforcement actions, including potential public notices, criminal charges, and sanctions, which could help ensure accountability and some redress for the victims.

43. These actions would be consistent with U.S. domestic law, as well as the United States' international human rights obligations, such as the International Covenant on Civil and Political Rights (ICCPR),[48] which the United States ratified in 1992,[49] and which guarantees the

[48] Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[49] Available at https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en.

protection of the right to privacy and the freedoms of expression, peaceful assembly and association, and political participation.

44. This will also be in line with the United States' domestic policies, such as calling out governments for "abusing technological advancements to infringe on the democratic process and on the human rights of their constituents"[50] and protecting civil society from cyber threats,[51] as well as its international commitments, priorities, and engagements related to defending free and secure internet. For example, as a founding member of the Freedom Online Coalition (FOC), which is a coalition of 40 governments that work together and engage with civil society and the private sector to support internet freedom, the United States has led on a number of statements aimed at protecting civil society from threats like STAR BLIZZARD.[52] In October 2023, during the 54th session of the UN Human Rights Council, acting as chair of the FOC, the United States presented a Joint Statement on the Heightened Risks Associated with Surveillance Technologies and the Importance of Safeguards in the Use of These Tools.[53] The statement builds on the FOC's March 2023 Guiding Principles on Government Use of Surveillance Technologies,[54] and calls on governments to take steps to ensure the use of these technologies is lawful and responsible, in accordance with states' domestic law and international obligations and commitments.[55] Similarly, in its 2020 Joint Statement on the Human Rights Impact of Cybersecurity Law, Practices and Policies, the FOC recommended that states "develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to

[50] Available at https://www.state.gov/commemorating-the-international-day-of-democracy-3/.
[51] Available at https://www.cisa.gov/news-events/alerts/2024/05/14/cisa-and-partners-release-guidance-civil-society-organizations-mitigating-cyber-threats-limited.
[52] Available at https://freedomonlinecoalition.com/.
[53] Available at https://freedomonlinecoalition.com/joint-statement-heightened-risks-associated-with-surveillance-technologies-and-the-importance-of-safeguards-in-the-use-of-these-tools/.
[54] Available at https://freedomonlinecoalition.com/guiding-principles-on-government-use-of-surveillance-technologies/.
[55] Available at https://freedomonlinecoalition.com/joint-statements/.

minimize potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists."[56] Previous FOC work, endorsed by the U.S. government, emphasized that such national law and policies should consider "the disproportionate threats faced by individuals and groups at risk" and "protect and promote human rights.[57] Other U.S.-led initiatives, like the Summit for Democracy, put human rights and democracy at the heart of the U.S. foreign policy.[58]

45. An effective enforcement action by this court would send a strong signal to the adversaries and allies alike that the United States will not tolerate threat actors like STAR BLIZZARD using U.S.-based infrastructure to target human rights defenders and journalists and destroy human rights, democracy, and the civic space. The court must help protect the rights and liberties of the civil society individuals that risk their lives daily to protect the values that the United States champions at home and abroad.

46. Finally, an enforcement action would also reward the courageous civil society victims for coming forward, allowing organizations like Access Now and the Citizen Lab to investigate the STAR BLIZZARD attacks against them, and sharing their stories and the impact that the attacks has had on them. Seeing a direct and concrete action from the US courts will also encourage other victims to speak out.

47. In the words of one of the STAR BLIZZARD's civil society victims, we "implore the court to consider the gravity of this attack [and] the lasting harm[s] it has caused" and to urgently address these harms.

[56] Available at https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf.

[57] Available at https://freeandsecure.online/recommendations/.

[58] Available at https://www.state.gov/further-information-the-summit-for-democracy/.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 23rd day of September, 2024, in Nuremberg, Germany.

____

Natalia Krapiva

Senior Tech - Legal Counsel
Access Now

EXHIBIT 1

Natalia Krapiva J.D.

Berlin, Germany ✉ natalia@accessnow.org Linkedin

SUMMARY

✔ Highly confident and skilled legal practitioner bringing 8+ years of increasingly responsible legal experience with US and international organizations and a passion for litigation, international human rights, and technology policy issues.

✔ Expert understanding of human rights law and practice, the international political system, and the internet. Proven ability to identify emerging issues and use legal mechanisms to prevent and mitigate threats.

✔ Recognized by senior management as a strategic and creative thinker who can provide expert and tactical advice to the organization, the team, and management.

✔ Demonstrable ability to manage competing and urgent tasks, as well as long-term and sustained projects, taking them all to completion while regularly reporting on progress to relevant stakeholders.

✔ Extensive portfolio of successful legal briefs, written publications, and press interviews.

✔ Juris Doctor (UC Berkeley), licensed in New York (USA), bilingual fluency in English/Russian and basic German.

PROFILE

❖ **Results Oriented:** Led successful business and human rights advocacy campaigns including against Sandvine (the company withdrew from Belarus and was added to the Entity List by the US Treasury Department) and Cellebrite (the company had to provide information to the US SEC on human rights risks of its technologies).

❖ **Ability to Analytically Solve Issues:** Analyzed court decisions and drafted multiple motions, expert opinions, and amicus brief, including the successfully filed amicus brief in the WhatsApp v. NSO 9th Circuit case, highlighting for the court the human rights implications of commercial spyware and its impact on victims.

❖ **Litigation and Investigation Experience**: Worked on over 300 cases as an Assistant District Attorney, ranging from minor assaults and DUIs to human trafficking and felony assaults, including working with victims and witnesses, preparing subpoenas, and appearing in court. As a Senior Tech-Legal Counsel, drafted and submitted over 20 legal filings on issues related to spyware, internet shutdowns, business and human rights, among others. Led and provided legal assistance to investigations of state-sponsored spyware attacks in El Salvador, Armenia, Serbia, EU, and beyond, including working with victims, media, and all the relevant stakeholders.

EMPLOYMENT EXPERIENCE

Access Now, Berlin, Germany **May 2019 – Present**

Defends and extends the digital rights of people and communities at risk

Senior Tech-Legal Counsel

- Work with the Digital Security Helpline to prevent and mitigate legal obstacles to its work, to its beneficiaries' work, and to the greater digital security ecosystem.
- Serve on the Legal team to shape Access Now's strategic direction and other accountability efforts, including thorough forensic investigations and strategic and impact litigation by Access Now and its partner organizations.

- Develop, support and represent Access Now in global partnerships and coalitions, such as global network of impact litigants, and identifying opportunities to promote new jurisprudence to better protect users at risk and advance digital rights under law.
- Serving as advisor to the General Counsel on external issues, including legal risks.
- Contributing to information gathering and norm development activities by Access Now's Policy and Advocacy team, including through input into blog posts, legal briefs, reports, and other written documents, ensuring they are appropriately informed by risks and threats to Access Now's mission.

Kings County District Attorney's Office, Brooklyn, NY — October 2018 – May 2019

Assistant District Attorney

- Analyzed assigned cases, prepared cases for trial, and appeared in criminal court.
- Interviewed witnesses, victims, and police officers to collect evidence and to make critical decisions to support court proceedings.

UC Berkeley School of Law Human Rights Center, Berkeley, CA — September 2016 - May 2018

Promotes human rights and international justice worldwide

Human Rights Investigations Lab Intern/Mentor/Legal Advisory Board Member

- Conducted cutting-edge open-source investigations into human rights and criminal law violations.
- Provided mentorship and guidance to students and management on legal and ethical matters and helped inform investigative strategies and future Lab projects.

Independent Research — July 2017 - May 2019

Research Assistant

- Assisted the former Benetech Vice President for Human Rights in advising on the digital needs of the newly-established United Nations International, Impartial and Independent Mechanism on Syria, by researching innovative ways of conducting investigations.

Queens County District Attorney's Office, New York, NY — May 2017 - July 2017

Legal Intern, Homicide Trials Bureau

- Assisted Homicide Trials Assistant District Attorneys in all stages of trials by conducting legal and factual research and drafting court motions.

Office of the UN High Commissioner for Human Rights, Geneva, CH — Jan 2017 - April 2017

Intern, Legal Policy Office

- Assisted senior staff in drafting, reviewing, and editing legal documents, including amicus briefs and human rights reports.
- Researched and wrote comprehensive memos on complex and/or novel issues of International Humanitarian Law (IHL), International Human Rights Law (IHRL) and International Criminal Law, including the relationship between IHL and IHRL, rights of children in armed conflict, and non-state armed groups.

UC Berkeley International Human Rights Law Clinic, Berkeley, CA — Sept 2016 - Dec 2016

Clinical Intern

- Conducted fact and international legal research contributing to the drafting of a report on the issue of Sexual Exploitation and Abuse (SEA) in United Nations Peacekeeping Missions used to advocate for SEA victim redress.

Natalia Krapiva J.D.

International Criminal Tribunal for the Former Yugoslavia, The Hague May 2016 - Aug 2016

Legal Intern, Office of the Prosecutor, Trial Division

- Conducted legal and factual research, analyzed evidence and assisted trial attorneys with drafting and revising the Final Trial Brief and court motions for the Prosecutor v. Mladić case.

Manhattan District Attorney's Office, New York, NY January 2014 - July 2015

Legislative Analyst, Division of Legislative Affairs

- Conducted extensive research on the Apple/Google encryption and other legislative issues, convened NYS law enforcement stakeholders, and wrote comprehensive briefings for the DA.

Mobilization for Justice (MFY Legal Services), New York, NY February 2013 - January 2015

Disaster Response Legal Services Assistant

- Worked closely with Disaster Response Law Project attorneys on a range of tasks, which helped victims of Hurricane Sandy, including conducting client intakes, reviewing and organizing documents and databases, filing FEMA and insurance appeals, and filing complaints against contractors with relevant governmental agencies.

New York State Attorney General's Office, New York, NY January 2012 - June 2012

Intern

- Assisted the Bureau Chief with various projects and initiatives related to combating human trafficking including staff training, outreach, advocacy, and funding.

United States Senator Kirsten E. Gillibrand's Office, New York, NY January 2012 - March 2012

Casework Intern

- Assisted constituents with Social Security, Medicare, Medicaid, Education, SNAP, HEAP, and FEMA issues.

NYS DOL Division of Compliance & Education, New York, NY June 2011 - August 2011

Summer Intern

- Conducted legal research and research on immigrant community organizations and coalitions across the state to help the former Division of Immigrant Policies & Affairs to better serve immigrants.

OTHER RELEVANT EMPLOYMENT, INTERNSHIPS, & VOLUNTEER EXPERIENCE

East Bay Community Law Center, Berkeley, CA	**April 2016**
Jewish Family & Vocational Service, Milltown, NJ	**February 2013 – March 2013**
Columbia University, New York, NY	**June 2010 – May 2011**
NJ Department of Labor, New Brunswick, NJ	**July 2008 – July 2009**
Middlesex County College, Edison, NJ	**September 2006 - April 2008**

EDUCATION

The University of California, Berkeley, School of Law, J.D. **2018**

International Law Certificate

Concentration: International Law

Human Rights and Technology Project: Conducted detailed research of cases where the International Criminal Court used open-source evidence, including Facebook and YouTube content, contributing to the Yale Law Journal publication by the Project supervisor.

Law Review: Wrote a research paper, published in the California Law Review, providing recommendations to the newly established International, Impartial, and Independent Mechanism on Syria to better utilize open source and clandestine documentary evidence.
Student Leader: International Human Rights Workshop, Central African Republic Project
Recipient: Herma Hill Kay Fellowship Award for Advancing Interests of Women in the Law and Elizabeth & Charles Tigar Public Interest Scholarship

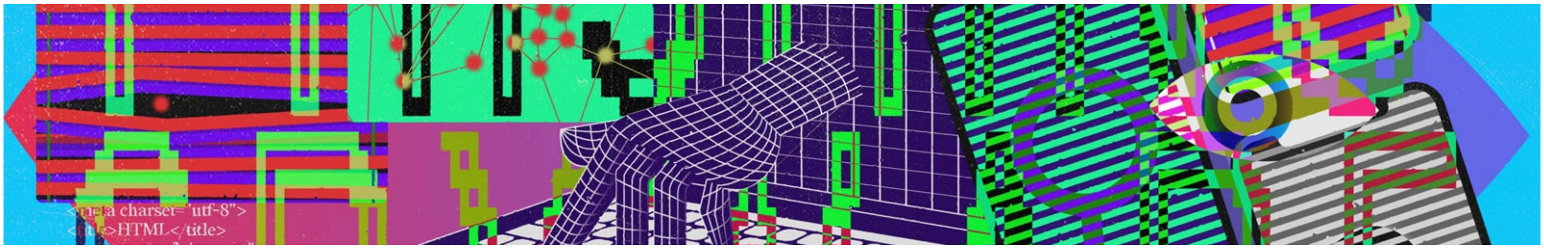
Columbia University, New York, NY **2012**
B.A. in Political Science, Dean's List, Summa Cum Laude 3.9 GPA
Concentrations: International Relations, American Politics
Recipient: Arthur Ross Foundation Award in Political Science
Member: Phi Beta Kappa, GS Honor Society

Middlesex County College, Edison, NJ **2008**
A.A. in Communication, A.A. in Education, Dean's List, Summa Cum Laude 3.9 GPA

EXHIBIT 2

FILED UNDER SEAL

EXHIBIT 3



Caught on the net: Russia-linked phishing campaigns ensnare Russian and Belarusian civil society, as well as international NGOs

PUBLISHED: 14 AUGUST 2024
LAST UPDATED: 15 AUGUST 2024

Access Now's Digital Security Helpline and the Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto ("the Citizen Lab"), in collaboration with First Department, Arjuna Team, and RESIDENT.ngo, have uncovered at least two separate spear-phishing campaigns targeting Russian and Belarusian nonprofit organizations, Russian independent media, international NGOs active in Eastern Europe, and at least one former U.S. ambassador. The Citizen Lab attributes one of the two campaigns to a known Russian threat group called COLDRIVER, with the other likely to be the work of a different, previously unnamed actor. Access Now and the Citizen Lab have dubbed this second actor "COLDWASTREL."

Spear phishing describes a highly personalized way of attacking victims, using carefully tailored information that aligns with a target's personal and professional experiences and activities. Based on Access Now and the Citizen Lab's assessment, it is likely that these threat actors or their sponsor organizations are still targeting civil society with spear phishing and other techniques. For more details on the Digital Security Helpline's investigation, read our full technical report.

READ THE FULL REPORT

// About COLDWASTREL

Our investigation into the first campaign began in March 2023, when Russian human rights organization First Department alerted us to a phishing email received by several international NGOs. The sender impersonated a staff member using the Proton Mail platform. First Department also reported that the same staff member's Proton Mail account had previously been targeted by a phishing attack in October 2022, resulting in them losing access to their account. In August 2024, we were again alerted by a previously targeted organization about a new phishing attack on their staff, which occurred in August 2024. Our Digital Security Helpline team investigated these cases, then reported them to Proton, ICANN, and other service providers.

While investigating the attacks, we discovered that an IP address used by the attacker was linked to domains impersonating several prominent civil society organizations active in Eastern Europe. We alerted the organizations in question, one of which confirmed they had received a similar phishing email, but preferred to stay anonymous for privacy and security reasons.

While some aspects of the attack indicate that the attacker, which we have dubbed "COLDWASTREL," may be acting in the interests of the Russian regime, we cannot confidently attribute the attack to a particular actor at this stage.

// About COLDRIVER

In early 2024, Access Now and the Citizen Lab identified a different cluster of phishing attacks. The organizations and individuals targeted in this campaign included Russian and Belarusian civil society organizations and independent media, international NGOs, and at least one former US ambassador. Citizen Lab has attributed this campaign to a Russia-based threat group COLDRIVER, also known as, among other names, STAR BLIZZARD, SEABORGIUM, and CALLISTO. You can read more about COLDRIVER in the Citizen Lab's investigation. According to several governments, this group is a subordinate of the Russian Federal Security Service (FSB)'s Centre 18.

// How the attacks were carried out

Below, we describe the pattern of the spear-phishing attacks we observed and offer guidance on how you can work to prevent or mitigate such attacks.

Both kinds of attacks were highly tailored to better deceive members of the target organizations. The most common attack pattern we observed was an email sent either from a compromised account or from an account appearing similar to the real account of someone the victim may have known. The phishing attacks were personalized to show scenarios that the individuals or their organizations might feasibly encounter in their daily work, mentioning topics such as event planning or financial discussions.

The attacks also typically included a seemingly locked PDF attachment, sometimes with a link purporting to help "unlock" the PDF's content, but which in fact led to fake login pages aimed at harvesting the target's information.

// The impact of the attacks

While some targets told us that they did not engage with the phishing emails described in the two attacks, others were deceived into entering their user credentials.

Even though we did not directly observe credentials being passed back to the attacker's infrastructure, it is likely that attackers were able to gain unauthorized access to some victims' email accounts.

If successful, such attacks could be enormously harmful, particularly to Russian and Belarusian organizations and independent media, since their email accounts are likely to contain sensitive information about their staff's identities, activities, relationships, and whereabouts. Any contact between Russian NGOs or independent media with Western-based organizations could be mischaracterized by the Russian government, and used as a pretext to designate them as a "foreign agent" or "undesirable organization." In some cases, this could even lead to individuals being criminally charged and imprisoned.

// How to protect yourself if you suspect you are being targeted

The following recommendations have been prepared jointly by Access Now and the Citizen Lab.

Start with prevention

Use two-factor authentication, correctly: Experts agree that setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked.

However, hackers like COLDRIVER and COLDWASTREL may try to trick you into entering your second factor; we have seen attackers successfully compromise a victim who had enabled 2FA. People using SMS messaging as their second factor are also at greater risk of having their codes stolen if a bad actor takes over their phone account.

We recommend that people use more advanced 2FA options such as security keys or, if they are Gmail users, Google Passkeys. Here are three guides for increasing the level of security for your account:

- Get Google Passkeys (Google)

- How to: Enable two-factor authentication (Electronic Frontier Foundation)
- Set up multi factor authentication (Consumer Reports)
- Use a security key (Consumer Reports)

Enroll in programs for high-risk users. Google and some other providers offer optional programs for people who, because of who they are or what they do, may face additional digital risks. These programs not only increase the security of your account, but also flag to companies that you may face more sophisticated attacks. Such programs include:

- Google Advanced Protection
- Microsoft Account Guard
- Proton Sentinel

Received a message? Be a five-second detective

- **Step one: check your inbox for the sender's email.** Ask yourself if you have received messages from this account before. COLDRIVER often uses lookalike emails to impersonate people known to the target either personally or professionally, so you may see an email that appears to come from someone you know, writing about something you would expect them to write about. Even if you have received previous messages from the same email address, it is possible to "spoof" a familiar looking email address, so move on to the next step.
- **Step two: check with the sender over a different medium**. If you have any concerns or are at all suspicious, do not open any PDF attachment or click on any link sent in the email. Instead, check directly with the purported sender, via another service, to confirm whether or not they've reached out to you. If you don't already have direct contact with them, consider asking someone you trust to inquire on your behalf.
- **Step three: don't just click.** Always consult an expert before opening a document you are unsure about. If you want to view a document that you think is probably safe, but want to take care, open the file *within* your webmail. Google, Microsoft, and others open the files on their computers and display the contents to you. This protects you from malicious code embedded in a document. But it **will not prevent you from clicking on potentially malicious links inside the document.**
    - If you are viewing an attached document inside your webmail, you should remain careful. **Don't just click on any links**; copy and paste them into your browser before visiting. Examine the domain carefully: Is it what you would expect for the site you expect to be visiting? Advanced phishing kits are very good at impersonating popular services, and often the only visual clue that it is not the authentic site will be in the address bar of the browser.
    - If you see a "login page" pop up, **stop**. This is a good time to consult a trusted expert.
- **Step four: beware of "encrypted" or "protected" PDFs.** This kind of message is almost always a cause for concern. Legitimately encrypted PDFs almost never include a single "click here" button inside the PDF, and they don't show a blurred version of the contents. Never click on any "login" links or "buttons" inside a PDF you have been sent.

Considering online virus-checking sites? You may wish to use online virus-scanning sites such as VirusTotal or Hybrid Analysis to check suspicious links or files.

- These services offer a useful service and can be part of a good security practice, but they come with a very important caveat: **when you use such free services, you are not the customer, you are the product.** Your files are available to many researchers, companies, and governments.
- We do **not** recommend using such tools to check "sensitive" files that may contain personal information or other private topics. Instead, contact a trusted expert that can help.

Think you are being targeted?

These recommendations address the kind of phishing that COLDRIVER and COLDWASTREL are currently using, but there are many other ways you could be targeted. Whatever your level of risk, we encourage you to get personalized security recommendations from the Security Planner, which also maintains a list of emergency resources and advanced security guides.

If you suspect that you have already been targeted in an attack, reach out to a trusted practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as partners, participants, grantees, and others. If this is the case, keep them informed about what has happened, what has been leaked, how this may impact them, and what steps you are taking to mitigate this impact.

If you believe you have been compromised: Access Now's Digital Security Helpline is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in nine languages, including Russian.

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts too. Consider using a password manager to keep track of multiple passwords.
- You can also review access logs on your accounts, such as Proton Mail's Authentication Logs, Gmail's Last Account Activity, and review devices with account access, as well as Microsoft's Check recent sign-in activity. Some users may still have questions after reviewing these logs. We encourage you to make a copy of the logs if you suspect you may have been targeted, to share with an expert for review.

NATALIA KRAPIVA

@natynettle

ACCESS NOW HELPLINE TEAM

@accessnow

EXHIBIT 4

SPEAR-PHISHING CASES FROM EASTERN EUROPE IN 2022-2024: A TECHNICAL BRIEF

accessnow

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

This paper is an Access Now publication. It is written by **Access Now's Digital Security Helpline team.** We would like to thank Natalia Krapiva, Senior Tech Legal Counsel at Access Now, who provided support for this brief. For more information, please visit: **https://www.accessnow.org**

Contact: **Hassen Selmi** | Incident Response Lead
hassen@accessnow.org

Published in August 2024

Spear-phishing cases from Eastern Europe in 2022-2024: a technical brief

In this technical brief, Access Now's Digital Security Helpline ("the Helpline") outlines forensic evidence for spear-phishing campaigns targeting civil society members from Eastern Europe and international NGOs working in the region. The analysis covers two separate campaigns documented between October 2022 and August 2024.

Our work highlights the key similarities between the campaigns, as well as their differences. The combination of the attack modalities, the profile of the victims, and other technical evidence points to the perpetrators being threat actors close to the Russian regime. The Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto ("the Citizen Lab") has confirmed that the attacks Access Now observed between April and June 2024 could be attributed to COLDRIVER. We also identified another cluster of attacks between October 2022 and August 2024 that were likely the work of a different actor, who does not appear to have been named previously and who we refer to as COLDWASTREL. We hope that the information provided will support civil society in raising awareness of the risks, further safeguarding their communications, and exercising further caution if they have a higher risk profile.

Additional context can be found in Access Now's blog post, "*Caught on the net: Russia-linked phishing campaigns ensnare Russian and Belarusian civil society, as well as international NGOs*."

Key findings

- Two spear-phishing campaigns targeted members of civil society from Eastern Europe and international NGOs working in the region. The campaigns are the work of two different threat actors, COLDRIVER and COLDWASTREL.
- The attacks used Proton Mail email addresses to impersonate organizations or individuals that were familiar or known to the victims.
- The attacks used PDF documents that appeared locked and provided a malicious link purporting to unlock them, but which instead led to fake login pages.
- The attacks were intended to mimic everyday scenarios regularly encountered by the targeted organizations, which work to defend and uphold human rights, thus underscoring the highly targeted nature of the campaign.

Campaign A: attacks by novel threat actor COLDWASTREL

A first set of attacks documented by the Helpline between October 2022 and August 2024 was likely the work of a threat actor that Access Now and the Citizen Lab have dubbed "COLDWASTREL."

The Helpline was first alerted to these attacks in March 2023. We learned that an unknown threat actor was using a Proton Mail address to impersonate a member of staff at a prominent Russian civil society organization, sending well-crafted emails to targets, including international NGOs.

The emails employed by the threat actor were designed to appear to come from an account well-known to the targets, modifying only one character to deceive those who would notice less subtle phishing attempts.

The modified characters were also carefully chosen to further dissimulate the deception. For example, the attacker replaced "s" with "c" before "k," which deflects attention both through use of phonetics and the similar physical appearance of the names when typed out.

Here's an example, using a pseudonym:

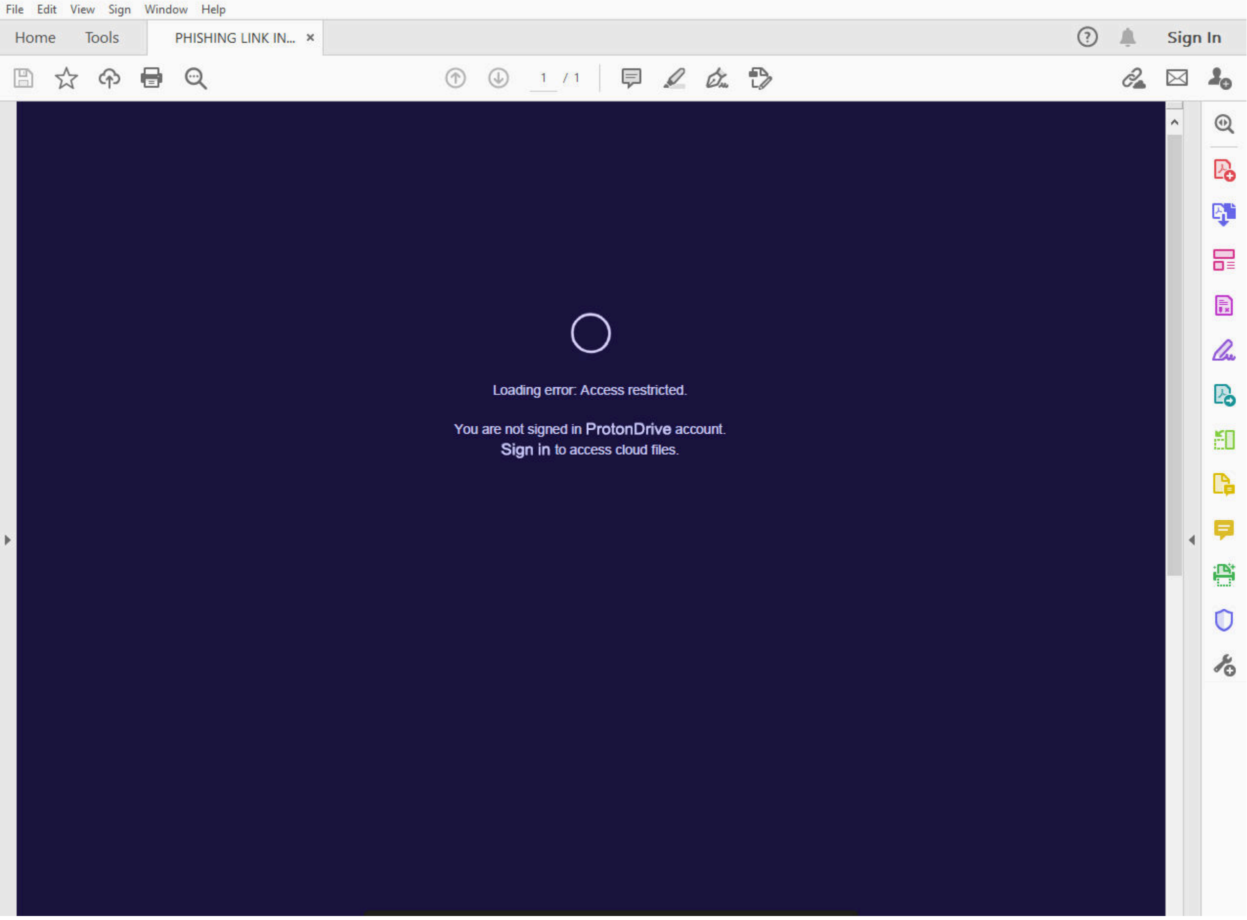
A real email address: Ivan.le**s**kovic@protonmail.com

A fake address used: Ivan.le**c**kovic@protonmail.com

The person whose account was impersonated in this manner was also targeted by a phishing attempt against their email that resulted in them losing access to their account. We believe that COLDWASTREL was also behind this attack.

Subsequent attacks in 2023 employed an alternative tactic. Attackers created a mail server with fake domains to impersonate an existing organization, including victims' actual partners and acquaintances. They combined this method with the use of aliases to appear familiar to the victims, using the one-character change method described above to deflect possible suspicion and make the attack harder to detect.

In some of the cases analyzed, the emails contained a PDF attachment which appeared to be locked. The same emails provided a link that purported to help unlock the PDF (see screenshot below).



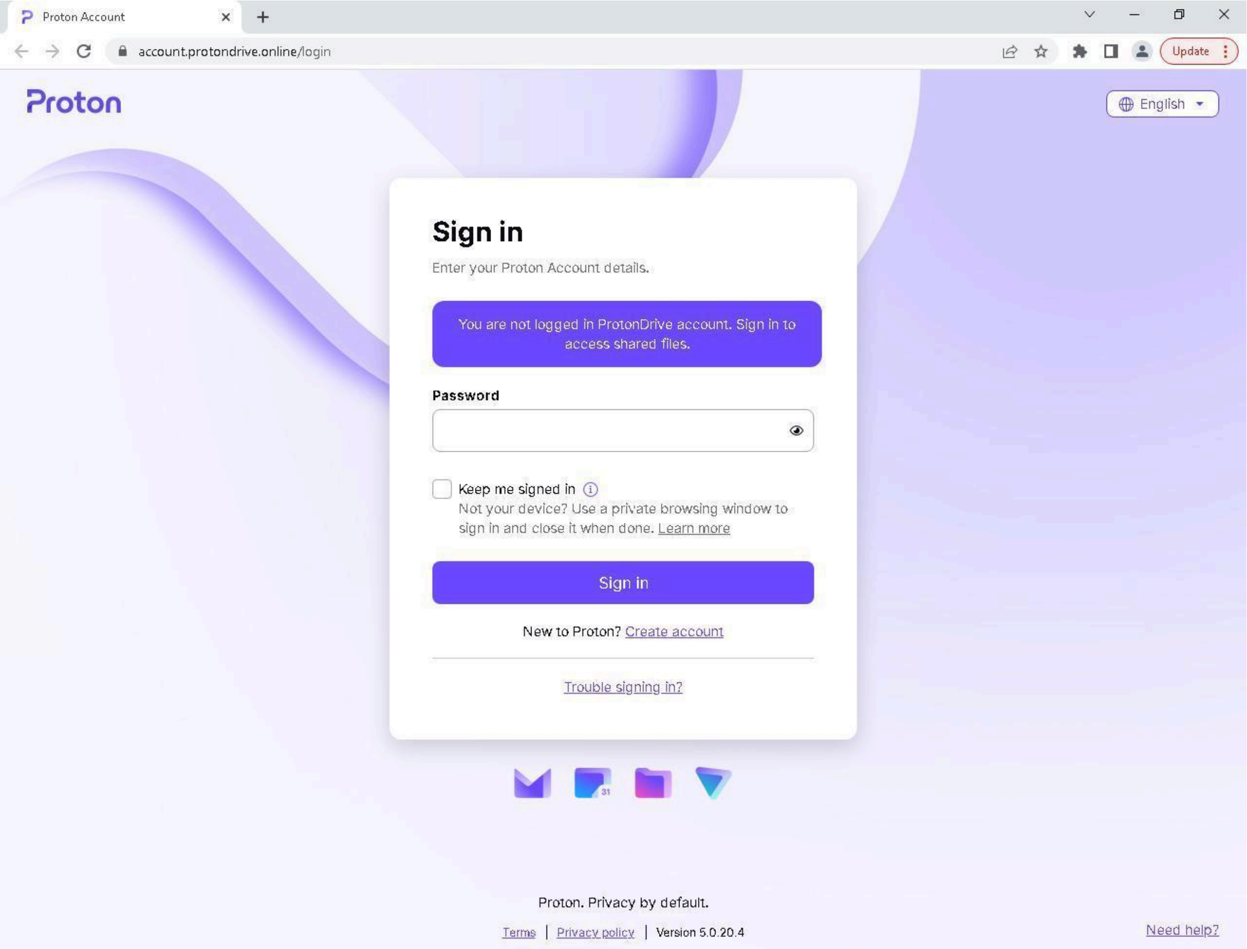
Loading error: Access restricted.

You are not signed in ProtonDrive account.
Sign in to access cloud files.

Sample of a PDF preview presented to targets as part of the COLDWASTREL campaign.

When followed, the link led to a fake Proton Mail login page. The Helpline was unable to verify any working links, as these appeared to have either been disabled or to have expired at the moment of analysis. However, in some cases, the fake login pages seemed able to harvest passwords and codes for two-factor authentication from the victims.

As a reference, see the screenshot below, shared by one victim, which includes a fake URL at the top (account.protondrive[.]online/login):



account.protondrive.online/login

Sign in

Enter your Proton Account details.

You are not logged in ProtonDrive account. Sign in to access shared files.

Not your device? Use a private browsing window to sign in and close it when done. Learn more

New to Proton? Create account

Proton. Privacy by default.

Terms | Privacy policy | Version 5.0.20.4

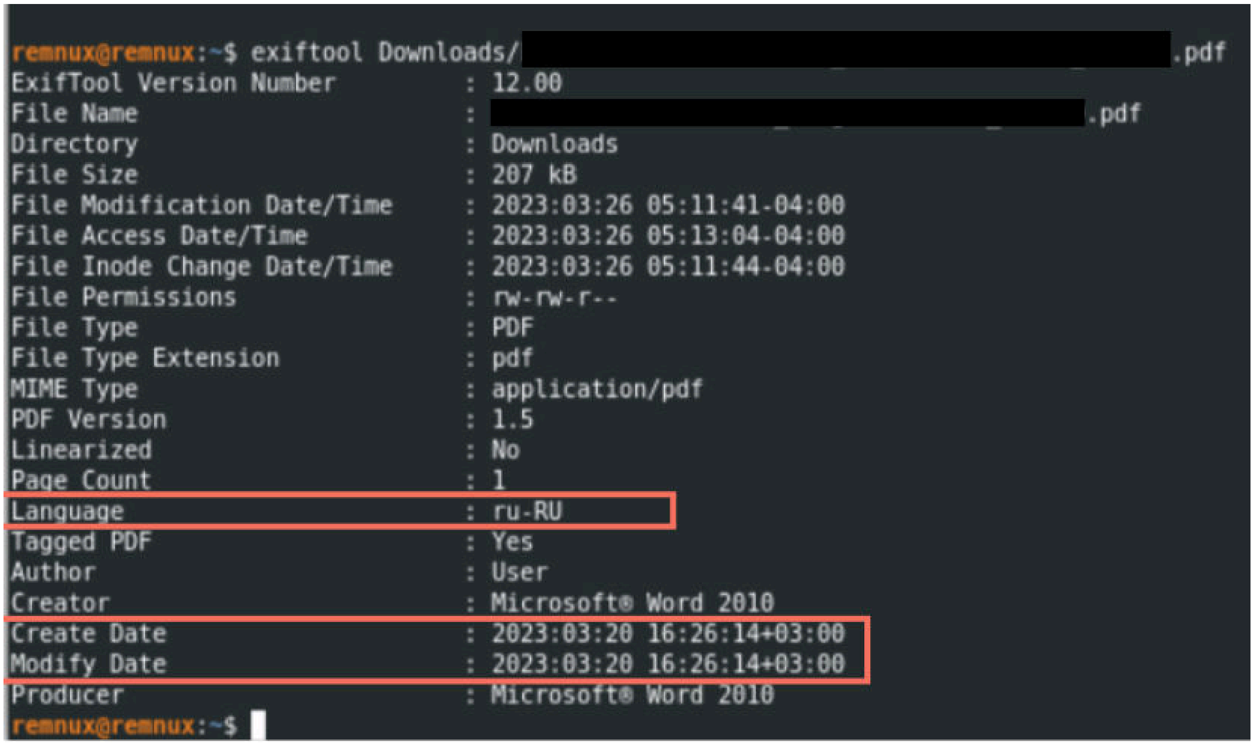
Sample of fake Proton Mail login page presented to targets as part of COLDWASTREL campaign.

Attackers' use of virtual private servers allowed the Helpline to identify and alert additional victims

By finding the virtual private servers that attackers employed in 2023 to host fake pages and email servers, the Helpline was able to identify other potential victims beyond those who initially sought our assistance, and to reach out proactively to alert them about the risk. At least one international human rights organization supporting civil society in the region confirmed that their staff were targeted with a similar campaign, although they did not share further details for analysis by the Helpline.

The Helpline believes that the threat actors behind this spear phishing campaign may be aligned with or close to the Russian regime. The victims are involved in human rights work in Russia, Ukraine, and across the region, which makes them of interest to the Kremlin. The attackers used context from activities that are highly relevant to the targets' work, such as references to funding and grant proposals. This reveals a profound understanding of the regional context and the targets' work, and a highly personalized attempt to exploit their vulnerabilities.

In addition, the analysis of the metadata included in the PDF documents deployed in the COLDWASTREL attacks showed the time of creation to have been GMT+3 (Moscow time) and the language to be ru-RU (Russian), as shown below. It should be noted that it is not definitive proof that the attackers are connected with Russia, since any attacker can change their computer time and language.



```
remnux@remnux:~$ exiftool Downloads/[redacted].pdf
ExifTool Version Number         : 12.00
File Name                       : [redacted].pdf
Directory                       : Downloads
File Size                       : 207 kB
File Modification Date/Time     : 2023:03:26 05:11:41-04:00
File Access Date/Time           : 2023:03:26 05:13:04-04:00
File Inode Change Date/Time     : 2023:03:26 05:11:44-04:00
File Permissions                : rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Page Count                      : 1
Language                        : ru-RU
Tagged PDF                      : Yes
Author                          : User
Creator                         : Microsoft® Word 2010
Create Date                     : 2023:03:20 16:26:14+03:00
Modify Date                     : 2023:03:20 16:26:14+03:00
Producer                        : Microsoft® Word 2010
remnux@remnux:~$
```

Output of exiftool shows a 2023 malicious PDF file creation time, time zone (GMT+3), and the system language (ru-RU).

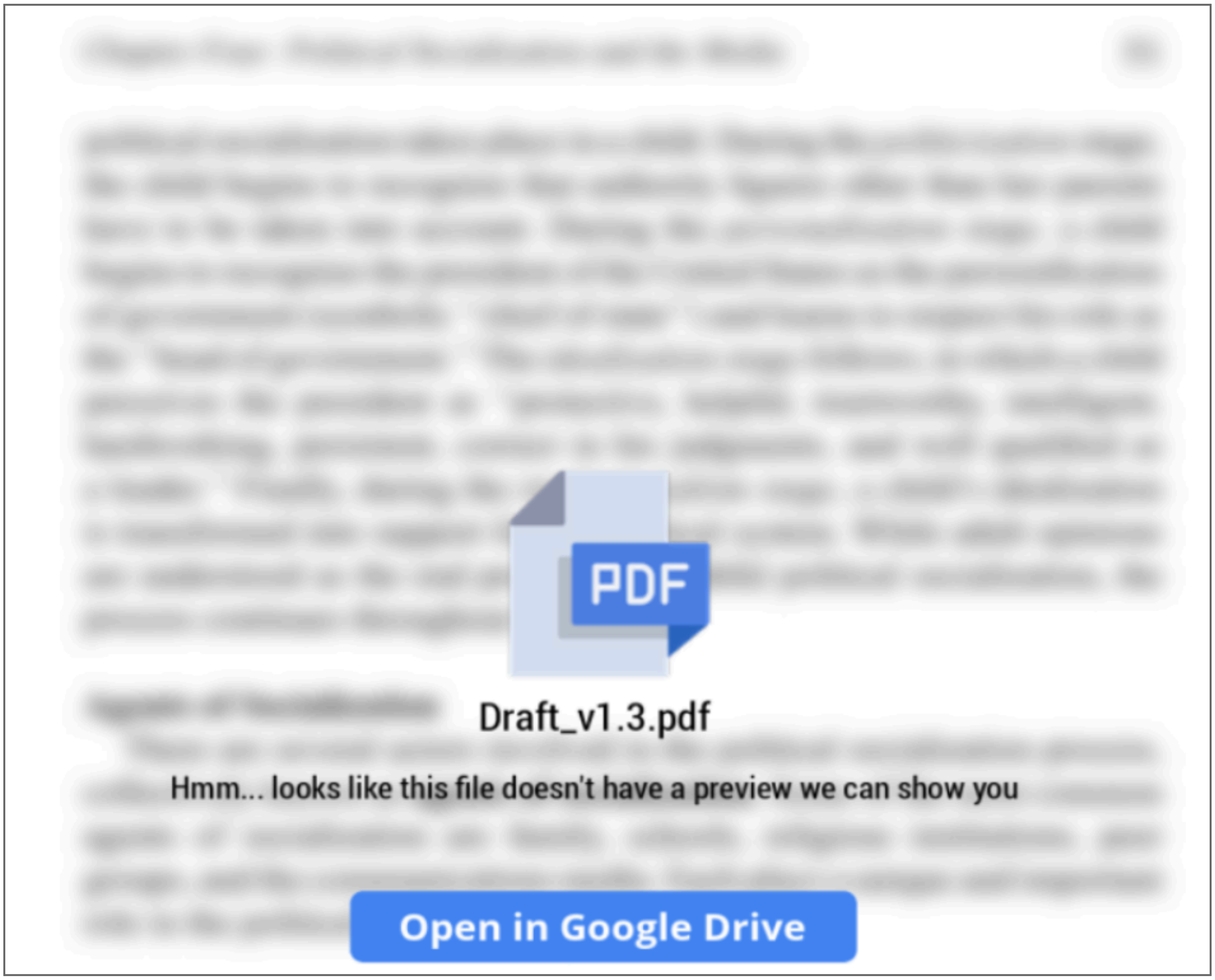
While some aspects of the attack indicate that COLDWASTREL may be acting in the interests of the Russian regime, we cannot confidently attribute the attack to any particular actor.

Readers should note that while finalizing this technical brief, we were alerted by one of the organizations previously targeted about a new phishing attack on their staff, which occurred in August 2024. Citizen Lab has tentatively concluded that COLDWASTREL is likely also the threat actor behind this latest attack.

Campaign B: attacks the Citizen Lab attributes to COLDRIVER

The spear-phishing campaign we observed in 2024 has some similarities with campaign A, such as reaching out to organizations working in Eastern Europe with a PDF containing malicious links.

The attackers also attempted to impersonate people that the victims knew, but this time, with mixed results. Some of the victims were suspicious about the communications received, recalling, for example, that they had not shared their contact details with the contact being impersonated, nor did the real contact have a Proton Mail address.



Draft_v1.3.pdf

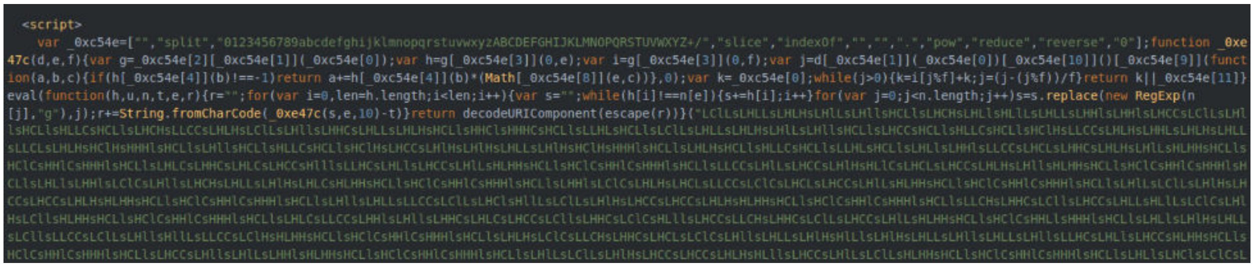
Hmm... looks like this file doesn't have a preview we can show you

Sample of the PDF preview presented to the targets as part of the COLDRIVER campaign.

The Helpline noted several other key differences in attackers' tactics and techniques. The attackers in the cases we observed between April and June 2024 used virtual private servers with Hostinger International Limited as their preferred host provider. However, we did not see any use of fake domains purporting to belong to real organizations, and we only analyzed instances where the attackers used Proton Mail email addresses to deliver their attacks. This made it harder to identify other potential victims compared with campaign A, for instance.

In addition, the links embedded in the campaign B PDF files included different mechanisms for validation, which is the process through which the code collects data from the target device, sends it to the server for processing, and offers different responses depending on what is analyzed.

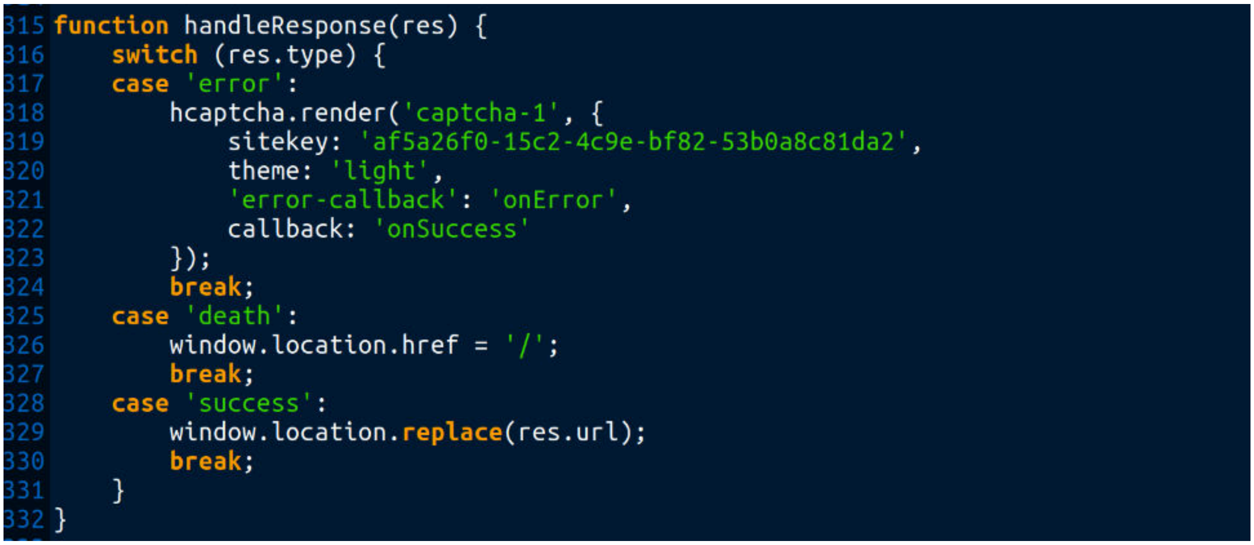
When Helpline analysts first visited these links, they observed an obfuscated code:



```
  <script>
    var _0xc54e=["","split","0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ+/","slice","indexOf","","",".","pow","reduce","reverse","0"];function _0xe
47c(d,e,f){var g=_0xc54e[2][_0xc54e[1]](_0xc54e[0]);var h=g[_0xc54e[3]](0,e);var i=g[_0xc54e[3]](0,f);var j=d[_0xc54e[1]](_0xc54e[0])[_0xc54e[10]]()[_0xc54e[9]](funct
ion(a,b,c){if(h[_0xc54e[4]](b)!==-1)return a+=h[_0xc54e[4]](b)*(Math[_0xc54e[8]](e,c))},0);var k=_0xc54e[0];while(j>0){k=i[j%f]+k;j=(j-(j%f))/f}return k||_0xc54e[11]}
eval(function(h,u,n,t,e,r){r="";for(var i=0,len=h.length;i<len;i++){var s="";while(h[i]!==n[e]){s+=h[i];i++}for(var j=0;j<n.length;j++)s=s.replace(new RegExp(n
[j],"g"),j);r+=String.fromCharCode(_0xe47c(s,e,10)-t)}return decodeURIComponent(escape(r))}("LClLsLHLLsLHLHsLHlLsLHllsHCLlsLHCHsLHLlsHLlLsLHLLsLHHlsLHHlsLHCCsLClLsLHl
lsHCLlsHLLCsHCLlsLHCHsLLCCsLHLHsLClLsLHllsLHHCsLHLLsLHLHsHCLlsHHClsHHHCsHCLlsLLHLsHCLlsLClLsLHLLsLHLHsLHlLsLHllsHCLlsLHCCsHCLlsHLLCsHCLlsHClHsLLCCsLHLHsLHHLsLHLHsLHLL
sLLCLsLHLHsHClHsHHHlsHCLlsLHllsHCLlsHLLCsHCLlsHClHsLHCCsLHlHsLHlHsLHLLsLHlHsHClHsHHHlsHCLlsLHLHsHCLlsHLLCsHCLlsLLHLsHCLlsLHLlsLHHlsLLCCsLHCLsLHHCsLHLHsLHlLsHLHHsHCLls
HClCsHHlCsHHHlsHCLlsLHLCsLHHCsLHLCsLHCCsHlllsLLHCsLHLlsLHCCsLHlLsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLLCCsLHlLsLHCCsLHlHsHLlCsLHCLsLHCCsLHLHsLHllsHLHHsHCLlsHClCsHHlCsHHHlsH
CLlsLHLlsLHHlsLClCsLHllsLHCHsLHLLsLHlHsLHLCsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHHlsLClCsLHLHsLHCLsLLCCsLClCsLHCLsLHCCsLHlLsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHlLsLClLsLHlHsLH
CCsLHCCsLHLHsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHllsLHLLsLLCCsLClLsLHClsHllLsLClLsLHlHsLHCCsLHCCsLHLHsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLLCHsLHHCsLClLsLHCCsLHLLsHLlLsLClCsLHl
HsLClLsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHLCsLLCCsLHHlsLHllsLHHCsLHLCsLHCCsLCllsLHHCsLClCsHLllsLHCCsLLCHsLHHCsLClLsLHCCsLHlLsHLHHsHCLlsHClCsHHLlsHHHlsHCLlsLHLlsLHlHsLHLL
sLCllsLLCCsLClLsLHllsHllLsLLCCsLClHsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHLHsLClCsLLCHsLHHCsLHCLsLClCsLHllsLHLLsLHlHsHlLlsLHlHsLHLLsLHllsLHLLsLHllsLLHCsLHLlsLHCCsHLHHsHCLls
HClCsHHlCsHHHlsHCLlsLHCCsLHllsLHlLsLHHlsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHlLsLClLsLHlHsLHCCsLHCCsLHLHsHLllsLHCCsLHlLsLClLsHLHHsHCLlsHClCsHHlCsHHHlsHCLlsLHLlsLHClsLClCsL
```

The JavaScript machine validation code is obfuscated using Hunter PHP Javascript Obfuscator.

The deobfuscation of this code shows an initial step, using a validation code, to check the victim's machine type, before delivering the web content. If the machine fails this check, the visitor is redirected to a generic landing page or to a Captcha page, which are clearly not harmful. This technique is used as an attempt to limit analysis and to allow only the malicious code to be served to the intended target.



```
function handleResponse(res) {
    switch (res.type) {
    case 'error':
        hcaptcha.render('captcha-1', {
            sitekey: 'af5a26f0-15c2-4c9e-bf82-53b0a8c81da2',
            theme: 'light',
            'error-callback': 'onError',
            callback: 'onSuccess'
        });
        break;
    case 'death':
        window.location.href = '/';
        break;
    case 'success':
        window.location.replace(res.url);
        break;
    }
}
```

Part of the deobfuscated code showing the function responsible for redirecting users based on the malicious server response.

Unfortunately, the Helpline could not proceed to the next stage of the validation or determine whether or not it succeeded. The code that determines the page's response is implemented inside a PHP file on the server side, which was inaccessible to analysts. The second stage could be either a fake login page, as used in the COLDWASTREL attacks, or a link to download malware.

The PDF samples from this campaign did not contain create or modify dates. The language was set as en-US (English) and the attackers used Western-sounding names for the author metadata. It is possible that the metadata was removed to avoid leaving traces that could be used for attribution.

The attack victims were Russian and Belarusian NGOs and independent media. The sharing of seemingly locked PDF files, along with links to "unlock" them, mirrors the strategy of attacks documented by Google's Threat Analysis Group (TAG), which they attribute to Russian threat actor COLDRIVER and which is confirmed by the Citizen Lab's analysis.

Conclusion: remain on high alert

While the attacks outlined in this report are not technically sophisticated, they rely on sophisticated social engineering methods in addition to techniques, such as the use of machine validation, omitting PDF metadata, and use of private hosting. These are measures that the attackers chose to reduce any detection surface.

The threat from these spear-phishing attacks remains high for civil society and journalists who are working to defend human rights with a focus on Russia and Eastern European countries. The main safeguard for them is high awareness of the risks, as well as careful treatment of all communications received.

The following recommendations have been prepared jointly by Access Now and the Citizen Lab.

Start with prevention

Use two-factor authentication, correctly: Experts agree that setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked.

However, hackers like COLDRIVER and COLDWASTREL may try to trick you into entering your second factor; we have seen attackers successfully compromise a victim who had enabled 2FA. People using SMS-messaging as their second factor are also at greater risk of having their codes stolen if a bad actor takes over their phone account.

We recommend that people use more advanced 2FA options such as security keys or, if they are Gmail users, Google Passkeys. Here are three guides for increasing the level of security for your account:

- Get Google Passkeys (Google)
- How to: Enable two-factor authentication (Electronic Frontier Foundation)
- Set up multi factor authentication (Consumer Reports)

- Use a security key (Consumer Reports)

Enroll in programs for high-risk users. Google and some other providers offer optional programs for people who, because of who they are or what they do, may face additional digital risks. These programs not only increase the security of your account, but also flag to companies that you may face more sophisticated attacks. Such programs include:

- Google Advanced Protection
- Microsoft Account Guard
- Proton Sentinel

Received a message? Be a five-second detective

- **Step one: check your inbox for the sender's email.** Ask yourself if you have received messages from this account before. COLDRIVER often uses lookalike emails to impersonate people known to the target either personally or professionally, so you may see an email that appears to come from someone you know, writing about something you would expect them to write about. Even if you have received previous messages from the same email address, it is possible to "spoof" a familiar looking email address, so move on to the next step.
- **Step two: check with the sender over a different medium**. If you have any concerns or are at all suspicious, do not open any PDF attachment or click on any link sent in the email. Instead, check directly with the purported sender, via another service, to confirm whether or not they've reached out to you. If you don't already have direct contact with them, consider asking someone you trust to inquire on your behalf.
- **Step three: don't just click.** Always consult an expert before opening a document you are unsure about. If you want to view a document that you think is probably safe, but want to take care, open the file *within* your webmail. Google, Microsoft, and others open the files on their computers and display the contents to you. This protects you from malicious code embedded in a document. But it **will not prevent you from clicking on potentially malicious links inside the document.**
    - If you are viewing an attached document inside your webmail, you should remain careful. **Don't just click on any links**; copy and paste them into your browser before visiting. Examine the domain carefully: Is it what you would expect for the site you expect to be visiting? Advanced phishing kits are very good at impersonating popular services, and often the only visual clue that it is not the authentic site will be in the address bar of the browser.
    - If you see a "login page" pop up, **stop**. This is a good time to consult a trusted expert.
- **Step four: beware of "encrypted" or "protected" PDFs.** This kind of message is almost always a cause for concern. Legitimately encrypted PDFs almost never include a single "click

here" button inside the PDF, and they don't show a blurred version of the contents. Never click on any "login" links or "buttons" inside a PDF you have been sent.

Considering online virus-checking sites? You may wish to use online virus-scanning sites such as VirusTotal or Hybrid Analysis to check suspicious links or files.

- These services offer a useful service and can be part of a good security practice, but they come with a very important caveat: **when you use such free services, you are not the customer, you are the product.** Your files are available to many researchers, companies, and governments.
- We do **not** recommend using such tools to check "sensitive" files that may contain personal information or other private topics. Instead, contact a trusted expert that can help.

Think you are being targeted?

These recommendations address the kind of phishing that COLDRIVER and COLDWASTREL are currently using, but there are many other ways you could be targeted. Whatever your level of risk, we encourage you to get personalized security recommendations from the Security Planner, which also maintains a list of emergency resources and advanced security guides.

If you suspect that you have already been targeted in an attack, reach out to a trusted practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as partners, participants, grantees, and others. If this is the case, keep them informed about what has happened, what has been leaked, how this may impact them, and what steps you are taking to mitigate this impact.

If you believe you have been compromised: Access Now's Digital Security Helpline is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in nine languages, including Russian.

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts too. Consider using a password manager to keep track of multiple passwords.
- You can also review access logs on your accounts, such as Proton Mail's Authentication Logs, Gmail's Last Account Activity, and review devices with account access, as well as Microsoft's Check recent sign-in activity. Some users may still have questions after reviewing these logs. We encourage you to make a copy of the logs if you suspect you may have been targeted, to share with an expert for review.

Annex: Selected indicators of compromise (some omitted for privacy and security reasons)

COLDWASTREL

Domains:
protondrive[.]online
service-proton[.]me
protondrive[.]me
protondrive[.]services

VPSes used:
185.247.224[.]39 (observed in the first quarter of 2023)
194.36.189[.]125 (observed in the third to fourth quarter of 2022)
91.196.70[.]47 (observed in the second quarter of 2023 to first quarter of 2024)
46.246.1[.]187 (observed in the first to second quarter of 2024)
38.180.86[.]201 (observed in the second to third quarter of 2024)
38.180.18[.]66 (observed in the second to third quarter of 2024)

PDF Samples:
4a9a2c2926b7b8e388984d38cb9e259fb4060cccc2d291c7910be030ae5301a3
a2bfc72714978a1b025717d8028168e91ebb10eeb576cd047990e960442c25ce
751496922cef7592d7bef6eff075c2531971a778d56bce50e1217bcdccabdd5b

COLDRIVER

Domains:
egenre[.]net
eilatocare[.]com
xsltweemat[.]org

PDF Samples:
0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e

EXHIBIT 5

THECITIZENLAB (https://citizenlab.ca)

Rivers of Phish

Sophisticated Phishing Targets Russia’s Perceived Enemies Around the Globe

By John Scott-Railton (https://citizenlab.ca/author/jsrailton/)[1], Rebekah Brown (https://citizenlab.ca/author/rbrown/)[2], Ksenia Ermoshina (https://citizenlab.ca/author/kermoshina/), and Ron Deibert (https://citizenlab.ca/author/profd/)

[1] Co-lead author [2] Co-lead author

August 14, 2024

Summary

- A sophisticated spear phishing campaign has been targeting Western and Russian civil society.
- This campaign, which we have investigated in collaboration with Access Now and with the participation of numerous civil society organizations including First Department (https://dept.one/), Arjuna Team, and RESIDENT.ngo (https://resident.ngo/), engages targets with personalized and highly-plausible social engineering in an attempt to gain access to their online accounts.
- We attribute this campaign to COLDRIVER (also known as Star Blizzard, Callisto and other designations). This threat actor is attributed to the Russian Federal Security Service (FSB) by multiple governments.
- We identified a second threat actor targeting similar communities, whom we name COLDWASTREL. We assess that this actor is distinct from COLDRIVER, and that the targeting that we have observed aligns with the interests of the Russian government.
- The Citizen Lab is sharing all indicators with major email providers to assist them in tracking and blocking these campaigns.

Click here (https://www.accessnow.org/russian-phishing-campaigns/) to read the Access Now Report and the Access Now Helpline Technical Brief. (https://www.accessnow.org/russian-phishing-technical-brief)

1. River of Phish: Campaign Overview

Our collaborative investigation with Access Now (https://www.accessnow.org/), with the assistance of multiple additional civil society organizations including First Department (https://dept.one/), Arjuna Team, and RESIDENT.ngo (https://resident.ngo/), has identified digital targeting using sophisticated spear phishing by this threat actor across multiple countries and sectors within civil society.

Observed Targets

The targets range from prominent Russian opposition figures-in-exile to staff at nongovernmental organizations in the US and Europe, funders, and media organizations. A focus on Russia, Ukraine, or Belarus is a common thread running through all of the cases. Some of the targets still live and work in Russia, placing them at considerable risk. Almost all targets that spoke with us and our investigative partner, Access Now, have chosen to remain unnamed and, for their privacy and safety, we are only including indicators from a limited selection of the cases that we have examined.

Polina Machold, Publisher of Proekt Media (https://www.proekt.media/en/home/) is among the targets, and we observed the attackers masquerading as an individual known to her. Proekt conducts high profile investigative reporting into official corruption and abuses of power in Russia. They are well known for high-profile reporting on Vladimir Putin, Ramzan Kadyrov, and other highly-placed Russian officials. Soon after their reporting into Russia's interior minister in 2021, they were declared (https://rsf.org/en/proekt-first-russian-media-outlet-be-declared-undesirable) an "undesirable organization" by the Russian Government.

We have also observed targeting of former officials and academics in the US think tank and policy space. For example, former US Ambassador to Ukraine, Steven Pifer was targeted with a highly-credible approach impersonating someone known to him: a fellow former US Ambassador.

We judge that these targets may have been selected for their extensive networks among sensitive communities, such as high-risk individuals within Russia. For some, successful compromise could result in extremely serious consequences, such as imprisonment or physical harm to themselves or their contacts.

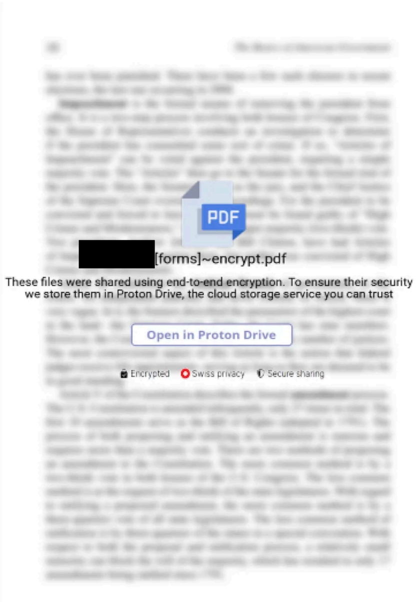
Importantly, we suspect that the total pool of targets is likely much larger than the civil society groups whose cases we have analyzed. We have observed US government personnel impersonated as part of this campaign, and given prior reporting about COLDRIVER's targeting, we expect the US government remains a target.

Typical Attack Flow: A Credible, Personalized Approach

The most common tactic we have observed is for the threat actor to initiate an email exchange with the target masquerading as someone known to them. This tactic includes masquerading as colleagues, funders, and US government employees. Typically, the messages contain text requesting that the recipient review a document relevant to their work, such as a grant proposal or an article draft.

In some cases, we have observed additional communication by the threat actor preceding or following the targeting message. Often highly and effectively personalized, this communication illustrates the depth of the threat actors' understanding of the targets. Multiple targets believed that they were exchanging emails with a real person.

We often observed the attacker omitting to attach a PDF file to the initial message requesting a review of the "attached" file. We believe this was intentional, and intended to increase the credibility of the communication, reduce the risk of detection, and select only for targets that replied to the initial approach (e.g. pointing out the lack of an attachment).



[redacted][forms]~encrypt.pdf

These files were shared using end-to-end encryption. To ensure their security we store them in Proton Drive, the cloud storage service you can trust

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/image8.png&nocache=1)

Figure 1: Screenshot of a purportedly-encrypted PDF lure. The phishing page is reached by clicking. (The screenshot has been slightly redacted to remove the name of an impersonated organization).

The email message typically contains an attached PDF file purported to be encrypted or "protected," using a privacy-focused online service such as ProtonDrive, for example. In fact, this is a ruse. When opened, the PDF displays what appears to be blurred text along with a link to "decrypt" or access the file. Actual ProtonDrive encryption looks substantially different (https://proton.me/support/send-large-files-proton-drive) from the River of Phish lures, suggesting that the attackers are relying on a general lack of awareness of what secure and encrypted document sharing looks like. In other cases, the blurred PDF includes text saying that a preview is not available, again soliciting a click.

While typical attacks were limited to a PDF, we also observed a few cases in which the attackers also sent an email crafted to appear as a document share, with the phishing link directly embedded in the email message. When one such case seemingly failed to generate a successful compromise, the attackers followed up with a PDF.

In some cases, the attackers followed up with targets that failed to enter their credentials with multiple messages asking if they had seen or "reviewed" the material. This approach, again, suggests a high degree of focus on particular targets.

If the Target Clicks

If the target clicks on the link, their browser will fetch JavaScript code from the attacker's server that computes a fingerprint of the target's system and submits it to the server (see: *Target Fingerprinting*). If the server elects to proceed with the attack, the server will return a URL, and the JavaScript code running in the target's browser will redirect the target there. If the server chooses, a CAPTCHA (from hCaptcha (https://www.hcaptcha.com/)) may be shown to the user prior to any redirect. The URL to which the target is redirected is typically a webpage crafted by the attacker to look like a genuine login page for the target's email service (e.g. Gmail or ProtonMail).

The login page may be pre-populated with the target's email address to mimic the legitimate login page. If the target enters their password and two-factor code into the form, these items will be sent to the attacker who will use them to complete the login and obtain a session cookie for the target's account. This cookie allows the attacker to access the target's email account as if they were the target themselves. The attacker can continue to use this token for some time without re-authenticating.

The use of a credible email ruse plus a PDF containing a phishing link is a favorite technique of multiple threat actors. Notably, PDF viewers built into webmail services like Gmail allow the recipient to click on hyperlinks within a PDF, and thus do not impede this attack.

2. River of Phish Campaign Infrastructure

First-Stage Domains

The first-stage infrastructure for this campaign involves phishing links embedded in the delivered PDFs, or sent in emails crafted to appear as document shares. The attackers typically register the domains and host the websites using Hostinger (https://www.hostinger.com/). Domains registered with Hostinger are hosted on shared servers which rotate IP addresses approximately every 24 hours, making the campaign more difficult to track. We did not identify any cases where a domain was operationally used within 30 days of its registration. This is a possible attempt to avoid being blocked by detection rules aimed at flagging emails or attachments with hyperlinks containing a recently registered domain.

Domain	Registration date	Date of Phishing email	Registrar	TLS Issuer
ithostprotocol[.]com	2024-01-16	2024-02-20	NameCheap	cPanel
xsltweemat[.]org	2024-03-14	2024-04-12	Hostinger	Let's Encrypt
eilatocare[.]com	2024-04-09	2024-05-29	Hostinger	Let's Encrypt
egenre[.]net	2024-05-19	2024-06-19	Hostinger	Let's Encrypt
esestacey[.]net	2024-05-19	2024-06-19	Hostinger	ZeroSSL
ideaspire[.]net	2024-05-20	2024-06-24	Hostinger	Let's Encrypt

Table 1: Examples of first-stage domains used in this campaign.

If the target clicks on the link in the PDF, the attack moves onto the next stage, which involves fingerprinting the user's system.

Target Fingerprinting

Each first-stage domain runs JavaScript code to fingerprint the target's browser and returns the fingerprint to the server, which decides how to proceed. Because we cannot see the server's code, we are not fully sure what the purpose of the fingerprinting is. However, because the server can elect to show a CAPTCHA to the target, we presume that the purpose of the fingerprinting may be to prevent certain automated tools from obtaining or analyzing the second-stage infrastructure, which contains the phishing page.

We did not directly observe the second stage of the attack or the credentials being passed back to the attacker's infrastructure; however, based on the targets' descriptions of the login page it is likely that the attackers leveraged a tool that is specifically designed to capture user credentials and enable unauthorized access, such as Evilginx (https://github.com/kgretzky/evilginx2) or another phishing platform. We note that COLDRIVER has been observed using Evilginx (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) in recent cases.

Our investigative partner, Access Now, has included a description of the fingerprinting code in their Technical Brief (https://www.accessnow.org/russian-phishing-technical-brief). The fingerprinting code was obfuscated using the Hunter PHP Javascript Obfuscator, a tool that is publicly available on GitHub (https://github.com/nicxlau/hunter-php-javascript-obfuscator).

Frequent Metadata Overlaps Across PDFs

PDFs associated with this campaign share consistent characteristics, including the location and formatting of the malicious link within the PDF, the PDF metadata, and the use of a fake English-language name that is different in each case for the PDF author. Based on the names identified in the PDFs, it appears that a name list such as this one (https://github.com/marcotcr/checklist/blob/master/checklist/data/names.json) or this one (https://github.com/FinNLP/humannames/blob/master/list.txt) was used in the generation of these names.

The chart below includes metadata from some PDFs that were shared directly with The Citizen Lab and Access Now.

A Selection of PDFs from the River of Phish Campaign

SHA256	Author Name	Producer	La
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d	Gracelyn Reilly	LibreOffice 7.0	en
0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88	Talon Blackburn	LibreOffice 7.0	en
efa2fd8f8808164d6986aedd6c8b45bb83edd70ca4e80d7ff563a3fbc05eab89	Howard Howe	LibreOffice 7.0	en
384d3027d92c13da55ceef9a375e8887d908fd54013f49167946e1791730ba22	Annabelle Kline	LibreOffice 7.0	en
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e	Paulina Mullen	LibreOffice 7.0	en
79f93e57ad6be28aae62d14135140289f09f86d3a093551bd234adc0021bb827	Emery Hogan	LibreOffice 7.0	en

Table 2: Examples of metadata details on malicious PDFs.

Target Phishing

In the cases we analyzed as part of this particular campaign, user credentials and associated two-factor authentication (2FA) tokens appear to be the primary targets of this phase of attack. We did not find any spyware delivered to target devices as part of this particular campaign. The focus on account access simplifies the attack infrastructure that is needed, as the attackers do not need to gain persistence or establish ongoing communications with the target's machine. It is important to note that the individuals and organizations targeted in this campaign likely face additional threats, such as spyware attacks (See here (https://citizenlab.ca/2024/05/pegasus-russian-belarusian-speaking-opposition-media-europe/), for example).

In January of 2024, Google's Threat Analysis Group (TAG) reported (https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/) on a custom malware backdoor called SPICA, which they assessed was the first known case of COLDRIVER developing and deploying custom malware. Similarly, we believe some of the targets who shared files with us may be regularly targeted by multiple threat actors and using multiple Tactics, Techniques, and Procedures (TTPs (https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html)). While this particular campaign did not leverage malware, we encourage human rights defenders, dissidents, journalists, and other members of civil society that may be targeted by Russian authorities to exercise extreme vigilance and contact experts such as Access Now's Digital Security Helpline (https://www.accessnow.org/help/) for help. We provide tips on how to identify suspicious communications below (See: *Protect Yourself & Your Colleagues*).

3. River of Phish: COLDRIVER Attribution

COLDRIVER is a Russia-based threat group attributed by several (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet#fsb-centre-18) governments (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a) to be subordinate to the Russian Federal Security Service (FSB) Centre 18 (*See: The Russian Cyber Espionage Landscape*, below). They have been active since at least 2019, possibly earlier, and their tactics primarily include very-involved social engineering and persona development. These personas are typically used to trick the target into visiting a malicious link, leading to the theft of their credentials, the bypassing of 2FA, and access to the target's information. This group has targeted widely in a pattern that aligns with Russian state interests, including targeting academia, NGOs, government institutions, and think tanks.

Selected Prior Reporting on COLDRIVER

Prior reporting on COLDRIVER describes strikingly similar tactics to the ones we see in this campaign. In 2017, cybersecurity firm F-Secure reported (https://web.archive.org/web/20170417102235/https://www.f-secure.com/documents/996508/1030745/callisto-group) on the activities of a group they tracked as "*Callisto group*", writing that they had tracked them since 2015. Their research highlighted the group's use of spear phishing (https://www.bbc.com/news/technology-39588703) to target "military personnel, government officials, think tanks and journalists." The attackers frequently impersonated legitimate websites and email addresses to trick targets into providing their credentials. At the time, F-Secure did not publicly attribute the group.

Company	Name assigned
F-Secure	Callisto group

Company	Name assigned
Microsoft	Star Blizzard / SEABORGIUM
Google TAG	COLDRIVER
PWC	Blue Callisto
Proofpoint	TA446
Sekoia	Calisto
Recorded Future	Blue Charlie
Mandiant	UNC4057

Table 3: One Threat Actor, Many Codenames.

In 2022, Microsoft reported on the group (https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/), which they track as *Star Blizzard* (previously *SEABORGIUM*). Google's Threat Assessment Group (TAG) (https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/) reported on them as *COLDRIVER*, PWC reported (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html#footnotes) on them as *Blue Callisto,* Proofpoint reported on them as TA446 (https://x.com/proofpoint/status/1618657863874015233), Sekoia reported (https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/) on them as *Calisto,* and Recorded Future reports on them as *Blue Charlie*. All research teams described similar tactics: elaborate spear phishing campaigns impersonating individuals known to the targets with the goal of stealing credentials to accounts and accessing sensitive information. In 2022, attribution was typically framed as "a likely Russia-based actor (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html)."

Attribution of COLDRIVER to the FSB in a Joint Governmental Advisory

In December 2023, government agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States issued a joint cybersecurity advisory (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a) detailing the activities of COLDRIVER. The advisory attributed the group to the FSB's Centre 18. The advisory notes that COLDRIVER's targets include "academia, defense, governmental organizations, NGOs, think tanks and politicians." The TTPs outlined in the advisory include extended target reconnaissance, the use of fake email and social media accounts, preference to target personal emails, the use of conference or event invitations as lures, the use of malicious domains impersonating legitimate organizations and more.

Attributing The River of Phish Campaign to COLDRIVER

Multiple TTPs and targeting from the River of Phish campaign closely align with public reporting on COLDRIVER. However, some of COLDRIVER's tactics (like lures using "encrypted" documents) share certain similarities with other threat actors. To increase our confidence, we sought to ensure that the River of Phish campaign matches multiple other research groups' COLDRIVER attribution. To that end, we approached Microsoft MSTIC, Proofpoint, and PwC, among others. Materials they shared enabled us to identify multiple direct overlaps between the River of Phish campaign and COLDRIVER. Finally, each independently confirmed that the activity we identified matched their own tracking of COLDRIVER. Together, this information suggests that the River of Phish campaign is attributable to the threat actor identified as COLDRIVER.

River of Phish Sample Overlap with Known COLDRIVER Campaigns

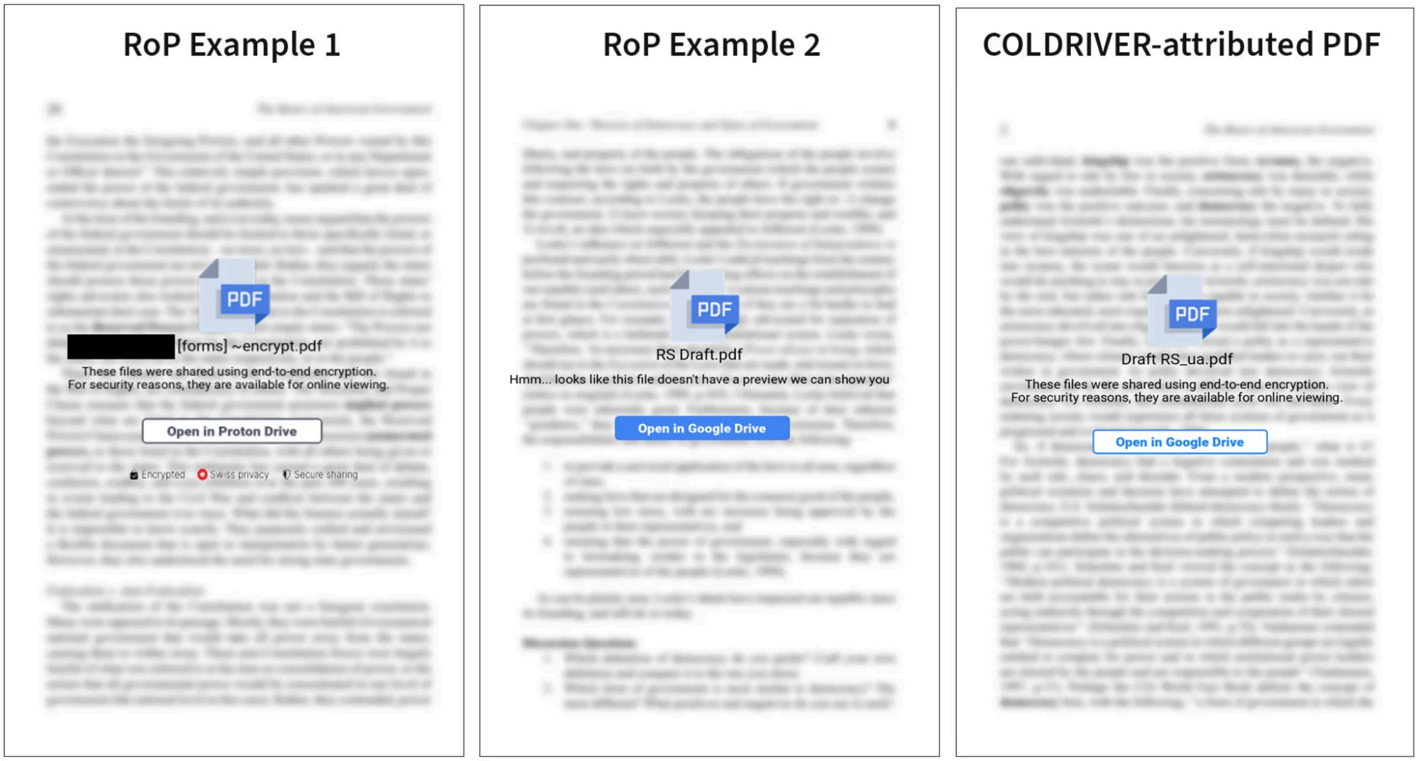
Proofpoint shared several publicly-available PDFs (on VirusTotal) with us that they attribute to COLDRIVER. Examination of these PDFs yielded multiple critical overlaps with the River of Phish campaign including: (a) matching bait PDF document structure and metadata and (b) overlapping phishing infrastructure.

Like the River of Phish ("RoP") PDFs (See: Table 2 above), those shared by Proofpoint included identical LibreOffice versions, seemingly-randomized author names, and en-US language settings.

Publicly-Available PDFs identified by Proofpoint as COLDRIVER			
c1fa7cd73a14946fc760a54ebd0c853fab24a080cbf6b8460a949f28801e16fc	Alexis Hill	LibreOffice 7.0	en-US
603221a64f2843674ad968970365f182c228b7219b32ab3777c265804ef67b0a	Carley Rivers	LibreOffice 7.0	en-US
df9d77f3e608c92ef899e5acd1d65d87ce2fdb9aab63bbf58e63e6fd6c768ac3	Haylie Wolf	LibreOffice 7.0	en-US

Table 4: Publicly-available COLDRIVER PDFs.

In addition to the PDF document metadata overlap, we observed substantial visual and content similarities in the PDFs. For example, RoP Example 1 shares bait text with this COLDRIVER-attributed text, and RoP Example 2 includes a variant on the filename used in the COLDRIVER-attributed PDF (See: Figure 2).



RoP Example 1

[redacted] [forms] ~encrypt.pdf

These files were shared using end-to-end encryption.
For security reasons, they are available for online viewing.

RoP Example 2

RS Draft.pdf

Hmm... looks like this file doesn't have a preview we can show you

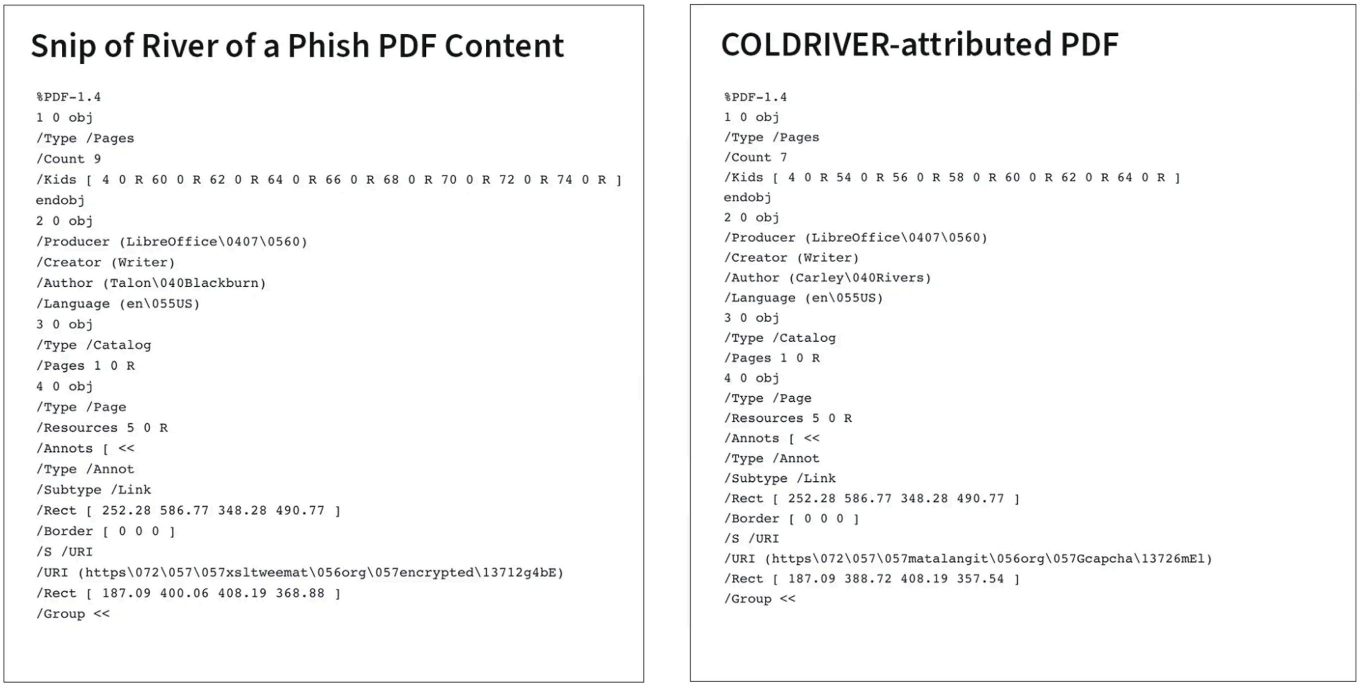
COLDRIVER-attributed PDF

Draft RS_ua.pdf

These files were shared using end-to-end encryption.
For security reasons, they are available for online viewing.

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure6-1.png&nocache=1)

Figure 2: Two River of Phish PDFs and one COLDRIVER PDF (Note: The Example 1 screenshot has been redacted to remove the name of an impersonated organization).



Snip of River of a Phish PDF Content

```
%PDF-1.4
1 0 obj
/Type /Pages
/Count 9
/Kids [ 4 0 R 60 0 R 62 0 R 64 0 R 66 0 R 68 0 R 70 0 R 72 0 R 74 0 R ]
endobj
2 0 obj
/Producer (LibreOffice\0407\0560)
/Creator (Writer)
/Author (Talon\040Blackburn)
/Language (en\055US)
3 0 obj
/Type /Catalog
/Pages 1 0 R
4 0 obj
/Type /Page
/Resources 5 0 R
/Annots [ <<
/Type /Annot
/Subtype /Link
/Rect [ 252.28 586.77 348.28 490.77 ]
/Border [ 0 0 0 ]
/S /URI
/URI (https\072\057\057xsltweemat\056org\057encrypted\13712g4bE)
/Rect [ 187.09 400.06 408.19 368.88 ]
/Group <<
```

COLDRIVER-attributed PDF

```
%PDF-1.4
1 0 obj
/Type /Pages
/Count 7
/Kids [ 4 0 R 54 0 R 56 0 R 58 0 R 60 0 R 62 0 R 64 0 R ]
endobj
2 0 obj
/Producer (LibreOffice\0407\0560)
/Creator (Writer)
/Author (Carley\040Rivers)
/Language (en\055US)
3 0 obj
/Type /Catalog
/Pages 1 0 R
4 0 obj
/Type /Page
/Resources 5 0 R
/Annots [ <<
/Type /Annot
/Subtype /Link
/Rect [ 252.28 586.77 348.28 490.77 ]
/Border [ 0 0 0 ]
/S /URI
/URI (https\072\057\057matalangit\056org\057Gcapcha\13726mEl)
/Rect [ 187.09 388.72 408.19 357.54 ]
/Group <<
```

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure7.png&nocache=1)

Figure 3: Comparing River of Phish and COLDRIVER PDF content.

Phishing Infrastructure Overlaps

In addition to the highly similar PDF content, phishing infrastructure linked from RoP bait PDFs showed substantial overlaps between the RoP campaign and COLDRIVER. The COLDRIVER-attributed PDFs contained links to multiple phishing domains (For example, See: Table 5).

Domain	Registration date	Registrar	TLS Issuer
togochecklist[.]com	2023-08-28	NameCheap	Let's Encrypt
vocabpaper[.]com	2024-03-15	Hostinger	Let's Encrypt
matalangit[.]org	2024-05-07	Hostinger	ZeroSSL

Table 5: Domain registration patterns and TLS issuers for known COLDRIVER PDFs.

The COLDRIVER phishing domain registration patterns exhibited similar characteristics to the ones we identified, such as registration using Hostinger and TLS certificates issued by Let's Encrypt or ZeroSSL.

Artifact	River of Phish	COLDRIVER
Domain Registrars	Namecheap, Hostinger	Namecheap, Hostinger, others

Artifact	River of Phish	COLDRIVER
TLS Certificate Issuers	ZeroSSL, Let’s Encrypt	ZeroSSL, Let’s Encrypt, others

Table 6: Comparing River of Phish and COLDRIVER domain registrars and TLS issuers.

In addition, reporting shared by PwC detailed recent COLDRIVER activity and validated our attribution of both PDFs and domains from this campaign.

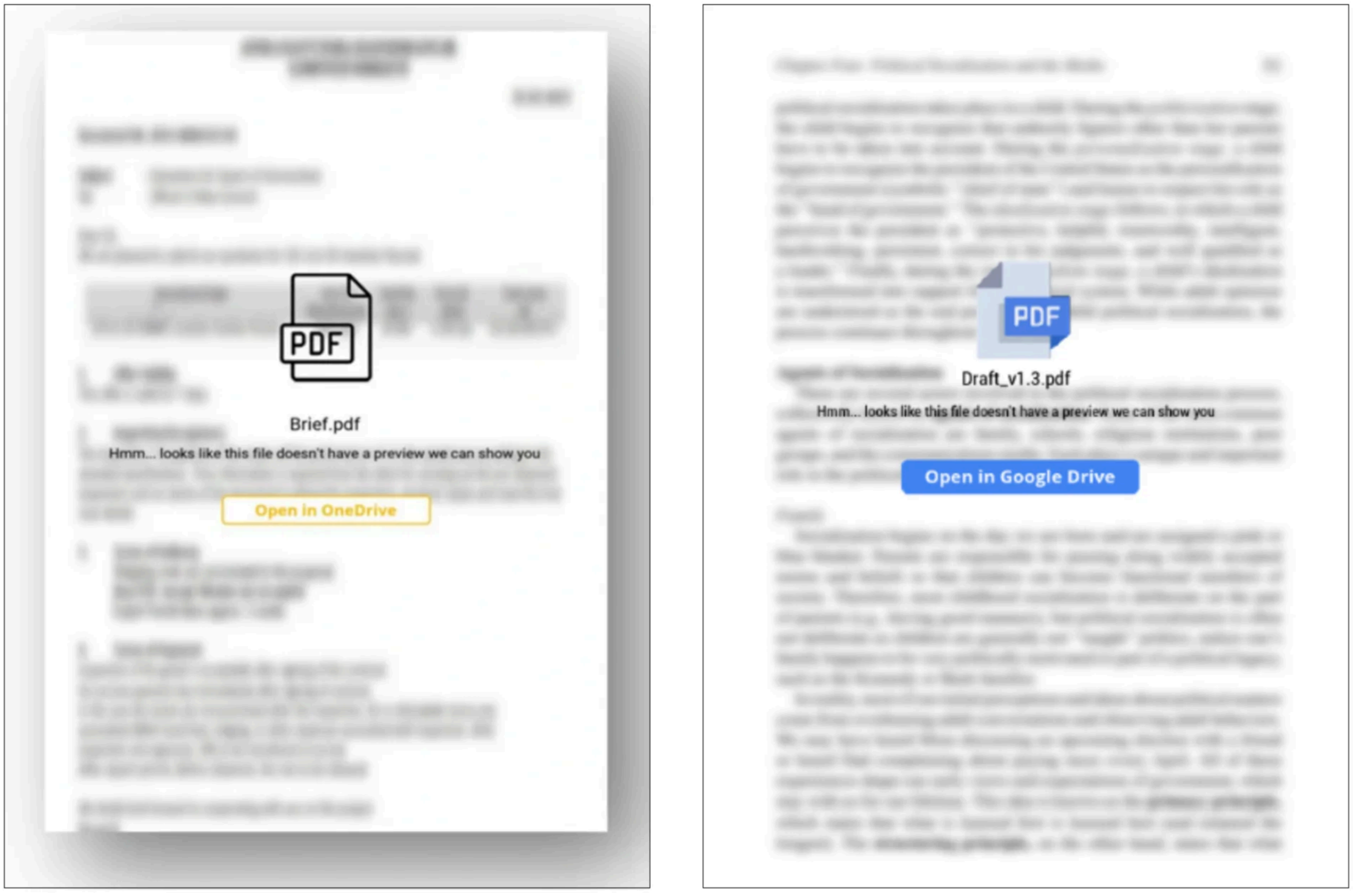
Additional TTP Overlap with Prior Public Reporting on COLDRIVER

Additionally, we noted that River of Phish employed a number of known TTPs of COLDRIVER.

The social engineering and spear-phishing delivery methodology remained consistent across past COLDRIVER activity and the current campaign we are tracking. These methods include:

- Impersonating a known individual by setting up a Proton Mail account using their name;
- Using information gained through reconnaissance to tailor the message in the initial email to make it look more authentic;
- Employing language indicating a desire to collaborate on a shared area of interest; and
- Using a fake password protected/encrypted PDF with the content blurred in the preview.

In one case, a RoP PDF features the text “*Hmm… looks like this file doesn’t have a preview we can show you*” (an error message shown by multiple Microsoft services when a file is not previewable) and a 2023 PDF from COLDRIVER features the identical text (Figure 4).



Hmm... looks like this file doesn't have a preview we can show you

Hmm... looks like this file doesn't have a preview we can show you

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure10.png&nocache=1)

Figure 4: PDF sent in a campaign reported by Microsoft in December 2023 (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) (left); PDF from the River of Phish campaign (right).

Finally, a PDF sent to one of the targets we examined contains multiple RoP elements, as well as an additional element previously associated with COLDRIVER. Specifically, the PDF contained an embedded link using a Customer Relationship Management (CRM) service previously reported as used by COLDRIVER, not a direct link to actor-registered infrastructure. In almost all other aspects, the document matched the RoP campaign. The PDF was sent in March 2024 and named “RS_version 1.3.pdf”. The email sender masqueraded as a retired US official seeking comment on a report on Ukraine. Language in the email describing a purported report and requesting a review was identical to other RoP emails. The attached PDF matched all RoP metadata, and the name used variants on “RS” and “Draft 1.3” naming observed in multiple RoP PDFs (See: *Figure 2*). However, unlike the other PDFs that included a direct link to a first-stage domain, this file included a link through HubSpot, a CRM provider.

```
dj-kqf04.eu1.hubspotlinksfree[.]com/Ctc…
```

In 2023 Microsoft identified COLDRIVER as a HubSpot user, and specifically noted (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) the practice of embedding HubSpot domains in the targeting PDF in an attempt to evade detection.

River of Phish: Signs of Continued Evolution?

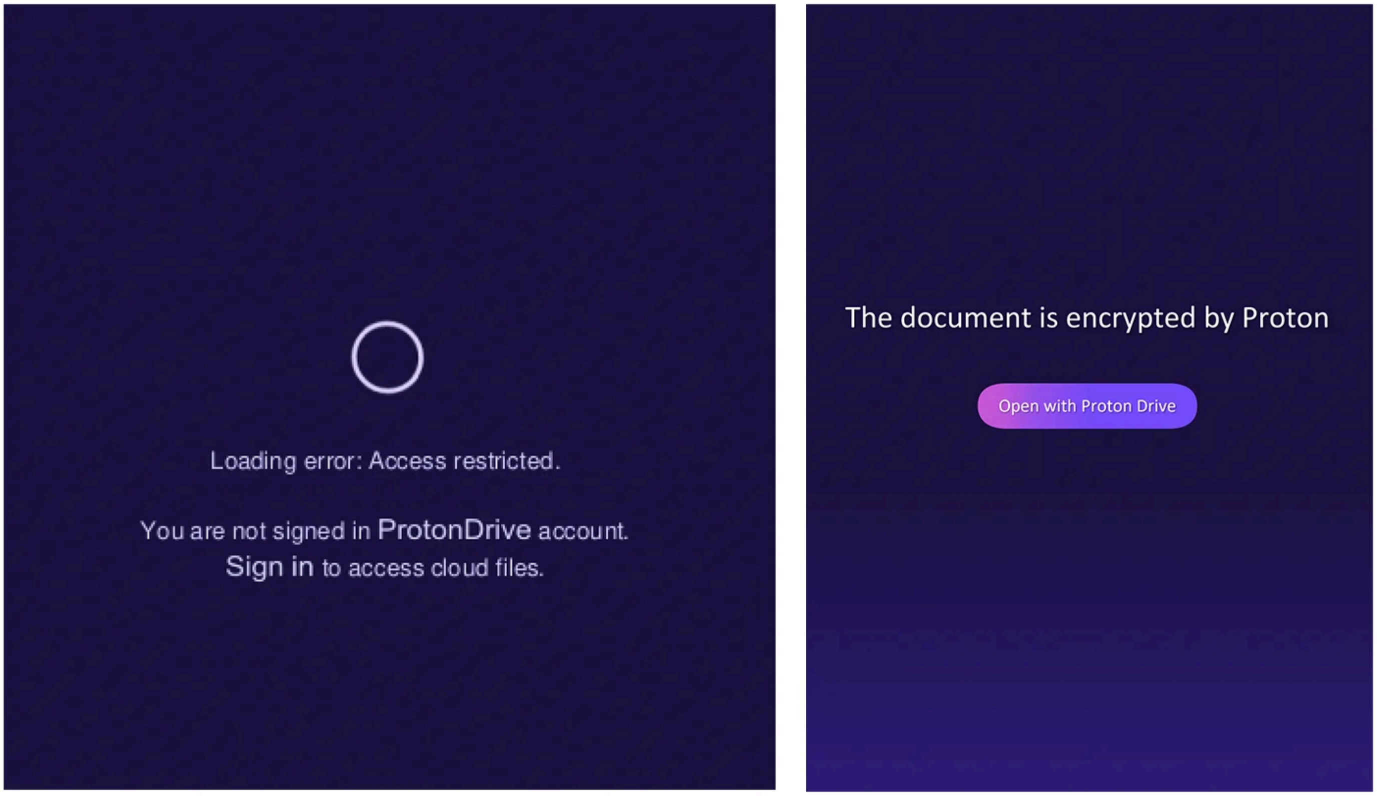
In addition to the previous use of HubSpot, earlier COLDRIVER reporting mentioned clusters of domains named around a particular theme or service being impersonated, such as *proton-docs[.]com*, *proton-reader[.]com*, and *proton-viewer[.]com* reported by Microsoft in 2022 (https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/). However both Microsoft (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) and Recorded Future (https://www.recordedfuture.com/research/bluecharlie-previously-tracked-as-tag-53-continues-to-deploy-new-infrastructure-in-2023) noted that COLDRIVER appeared to be using a "more randomized (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/)" domain generation mechanism starting in 2023, suggesting adaptation to previous detection techniques, and an effort to hide targets. RoP first-stage infrastructure did not include any themes in domain naming, however we note that our report focuses specifically on civil society clusters and thus it is possible that COLDRIVER is using other domain naming schemas against other targets.

Previous reporting also identified COLDRIVER domains registered through Namecheap. During this campaign we observed that the domain registrar of choice changed to Hostinger sometime between January and March of 2024. PwC reporting (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html#footnotes) highlighted that COLDRIVER has previously used Hostinger as a registrar in 2022, however more evidence is needed to determine whether this is a change that will persist across future COLDRIVER activity.

In addition to the analysis in this section, we have also developed a YARA rule (See: Appendix) that will assist other researchers in identifying other PDF files likely attributable to River of Phish / COLDRIVER.

4. COLDWASTREL: A New Threat Actor Surfaces?

In March 2023, our investigative partner Access Now began receiving cases of personalized phishing. The first were shared by the Russian human rights organization First Department. Access Now shared the cases with The Citizen Lab. Superficially, the messages had much in common with COLDRIVER. For example, the attacker sent PDF attachments with references to ProtonMail and ProtonDrive designed to trick targets into clicking on a link. However, close analysis revealed numerous differences, ultimately leading us to conclude that these were the work of a separate threat actor.



Loading error: Access restricted.

You are not signed in ProtonDrive account.
Sign in to access cloud files.

The document is encrypted by Proton

[(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure11.png&nocache=1)](https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/stitched-figure11.png&nocache=1)

Figure 5: Screenshots from COLDWASTREL PDFs.

Consistent Differences Between Bait PDFs

This campaign deviates in several important aspects from COLDRIVER, such as the characteristics of the malicious PDF (*see Table 7*) and front-end infrastructure. At this time, we assess that this activity cluster is not the work of the COLDRIVER operator and warrants further investigation.

	COLDRIVER	**COLDWASTREL**
PDF Version	1.4	1.5
PDF Language	en-US	ru-RU
PDF Author	Plausible-yet-obscure English language names	“User”
Links in PDF	Unique to each PDF	Consistent across mu
Links in PDF	Redirected to fingerprint, then to separate domain/site to gather credentials	Hosted the phishing

Table 7: Overview of differences in the PDFs and infrastructure between two campaigns that shared similarities in social engineering and credential harvesting.

Our colleagues at Access Now have identified an additional COLDWASTREL PDF on VirusTotal which we include here to assist other researchers in pursuing this threat actor.

COLDWASTREL PDF on VirusTotal

```
4a9a2c2926b7b8e388984d38cb9e259fb4060cccc2d291c7910be030ae5301a3
```

Infrastructure Differences

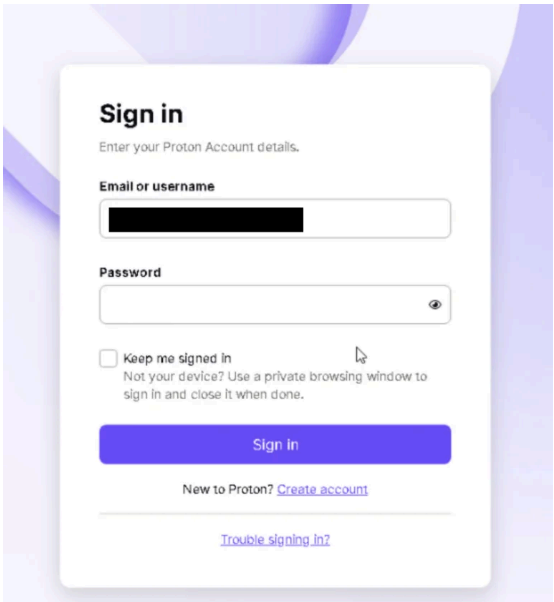
In addition to the differences in the PDF content and metadata, there were several other notable differences between the two attacks:

- All pre-2024 COLDWASTREL PDFs contained a link to the same domain, *protondrive[.]online*. This tactic deviates from the COLDRIVER activity that we investigated, which seemed to use a different domain for each PDF, without making use of a lookalike domain.
- The domain *protondrive[.]online* also differs from the infrastructure seen with COLDRIVER. The domain was registered through URL Solutions Inc, which deviates from the RoP/COLDRIVER TTPs described above.

Together with Access Now, we are referring to this operator as COLDWASTREL. We hope that other research teams will be able to advance this investigation further using indicators provided in Access Now's report (https://www.accessnow.org/publication/russian-phishing-campaigns/). While we are not attributing this campaign, and have only a limited number of targets, we note that the COLDWASTREL targeting that we have observed does appear to align with the interests of the Russian government.

Fresh COLDWASTREL?

Shortly prior to publication of this report, we have tentatively identified what appears to be renewed COLDWASTREL targeting, based on TTPs, targeting overlap and infrastructure similarity. In this attack, the decoy PDF included the domain *protondrive[.]me* which, when clicked, redirected to phishing hosted at *protondrive[.]services*.



Sign in

Enter your Proton Account details.

Email or username

[redacted]

Password

□ Keep me signed in

Not your device? Use a private browsing window to sign in and close it when done.

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/image1-1.png&nocache=1)

Figure 6: An August 2024 COLDWASTREL phishing page. The prepopulated email address of the target has been redacted.

5. Why Do Some Governments Still Phish?

Governmental threat actors, including in states that possess a high degree of technical competency (e.g. reserves of zero-day exploits), continue to phish *because personalized phishing still works*. When the cost of discovery remains low, phishing remains not only an effective technique, but a way to continue global targeting while avoiding exposing more sophisticated (and expensive) capabilities to discovery.

Threat actors like the FSB are equipped with substantial intelligence gathering and analytical capabilities. They possess a detailed window into potential targets' relationships and work activities which enables operators to craft very credible phishing lures. Research shows that phishing leveraging personal information has a much higher probability of success (https://www.sciencedirect.com/science/article/abs/pii/S0003687022002319), and we speculate that a mature phishing campaign against a longstanding target benefits from a positive feedback loop in which more cycles of phishing yield ever-more detailed information that can be used to create increasingly convincing lures for future victims.

Where we do see evolution and tactical cleverness from COLDRIVER, it remains just enough to bypass certain modes of discovery. For example, in the River of Phish campaign, we see a wide range of paired sender names, domains, and PDF metadata. It is possible that these pairings are each used for only a very small number of targets. This approach may indicate efforts to evade detection by popular email platforms.

As platform and endpoint security continues to thwart attacks, attackers must rely on increasingly sophisticated social engineering that can be hard to distinguish from normal communications. Confirming the authenticity of the message and sender will protect both parties, and is well worth the extra time and effort. As COLDRIVER's operators must know, this is not a practical action for every message.

Smash & Grab Phishing?

Numerous features of COLDRIVER's activities increase the chance of a successful compromise while also increasing the chance that a sophisticated target or analyst will identify the communications as malicious.

For example, impersonating an individual known to the target increases the likelihood of discovery because the target can usually contact the impersonated individual to inquire whether the communication is authentic. This chance of discovery is compounded by the use of a bait document ruse that is also likely to lead to puzzled victims, reports, and eventual discovery.

This sort of social engineering tactic is well suited to a persistent adversary that does not face reputational or criminal penalties from discovery. For example, the operators of COLDRIVER presumably enjoy the protection of the Russian government, and know better than to schedule a holiday at Disney World in Florida.

While the volume of past reporting on COLDRIVER has probably disrupted specific campaigns, it is unlikely to put a stop to their activity. Indeed, we see evidence that the operator makes minimal changes in their tactics in response to disruptions. Such changes buy them a modest window of time to continue targeting even though a degree of discovery, including further exposure by researchers and even governments, remains inevitable.

6. The Russian Cyber Espionage Landscape

Russia has a long history (https://us.macmillan.com/books/9780374287269/activemeasures) of espionage that reaches back to pre-Soviet times, and has engaged in cyber espionage campaigns and active cyber operations for decades (https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/). These operations have been extensively studied by academics (https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall), civil society (https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en) organizations, journalists (https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/), governments (https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf) and the commercial (https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/) cybersecurity (https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm) community. Generally, Russian cyber espionage and active cyber operations are undertaken independently by multiple (and sometimes competing (https://ecfr.eu/archive/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf)) state security agencies, occasionally with the participation of organized criminal groups (https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html) or other private sector entities (e.g., NTC Vulkan (https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/), RomCom (https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/), Cadet Blizzard (https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/)).

There are several Russian and Russian-aligned entities that undertake or are responsible for cyber espionage (see here (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet#cyber-operations-and-the-russian-intelligence-services)). Russia's foreign intelligence service, the SVR (*Sluzhba Vneshney Razvedki*), is responsible for foreign intelligence gathering and is generally known for long-term espionage campaigns such as those publicly referred to as APT29, "Cozy Bear" or "The Dukes." SVR-linked campaigns have typically involved (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a) accessing credentials of targeted entities through password spraying, brute forcing, and other means of accessing cloud and other accounts.

Russia's main intelligence directorate of the armed forces, the GRU, is associated with cyber espionage and cyberwarfare (https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c) operations designated as APT28, Fancy Bear, and Sandworm, and has been linked to DDoS (https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine) and disruptive malware (https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and) attacks (https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-greenberg/) on critical infrastructure, the financial sector, government and non-governmental organizations, and other sectors. The US, UK and other Western governments have also linked (https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF) this entity to the compromise of edge routers in order "to host spear-phishing landing pages and custom tools."

Meanwhile, Russia's FSB has responsibilities covering internal security, counterintelligence, and foreign espionage. Two units within the FSB, Centre 16 and Centre 18, are responsible for cyber espionage, with the activities of COLDRIVER falling under the umbrella of the latter. According to a UK government assessment (https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet#cyber-operations-and-the-russian-intelligence-services), Centre 18 is also known as the Centre for Information Security (TsIB) Military Unit 64829.

7. Civil Society Targeting by Russia: Always Present

Cyber espionage campaigns and active cyber operations targeting government entities, critical infrastructure, businesses and financial institutions have traditionally received the bulk of commercial cybersecurity firms' and media attention. However, this selection bias (https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658) arising from commercial priorities has produced a distorted view of the overall victim set. Until recently, attacks targeting civil society tended to be overlooked in industry and government reporting because civil society lacks the resources to pay for high-end services, which means that indicators that might be gleaned from civil society may be largely unseen by cybersecurity firms.

A major takeaway (https://targetedthreats.net/) of the last decade and a half of The Citizen Lab's research into digital espionage is that civil society is a major and often overlooked (https://circleid.com/posts/20130304_-civil_society_hung_out_to_dry_in_global_cyber_espionage/) segment, despite being targeted by the same groups that attack government and industry. Authoritarian governments are particularly sensitive to political opposition, dissidents and investigative journalism and routinely orient (https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert) their cyber espionage campaigns towards groups involved in those activities, both at home and abroad. Cyber espionage against civil society is also a major component of digital transnational repression (https://citizenlab.ca/2022/03/digital-transnational-repression-explained/), which has been growing in scope and scale worldwide.

In 2017, for example, The Citizen Lab published a report (https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/) detailing a Russia-aligned hack and leak operation, which we called "Tainted Leaks." The investigation detailed an extensive phishing operation targeting 200 unique individuals across 39 countries. Those targets included senior government and military officials, CEOs of energy companies, and civil society. We discovered that civil society targets, including academics, journalists, activists, and members of NGOs, represented the second largest cluster set (21%), after government officials. Although we could not attribute that operation to a single entity, there were several indicators suggesting links to APT28, a Russian threat actor affiliated with the GRU.

These cyber attacks targeting civil society are gaining wider visibility, thanks in part to the 10 plus years of reporting by The Citizen Lab, Access Now, Amnesty International, investigative journalists, and media consortia. The US, UK, Canada and other Western governments, as well as cybersecurity (https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023) firms (https://radar.cloudflare.com/reports/project-galileo-9th-anniv), have formally (https://www.cisa.gov/news-events/alerts/2024/05/14/cisa-and-partners-release-guidance-civil-society-organizations-mitigating-cyber-threats-limited) acknowledged (https://www.canada.ca/en/communications-security/news/2024/05/canada-joins-international-security-partners-in-release-of-advisory-guidance-on-growing-cyber-security-threat-to-civil-society.html) the frequency of and risks to civil society stemming from cyber espionage and cyber operations, now echoing civil society's reporting.

Other Digital Threats to Civil Society Groups Working On and In Russia

Civil society is under extreme threat in Russia. A recent study (https://jfj.fund/attacks-on-media-workers-in-russia-in-2021-2023/) conducted by the Justice for Journalists Foundation counts a total of 5,262 cases of attacks/threats against professional and civilian media workers and editorial offices of traditional and online media, as well as against Russian journalists abroad in 2021-2023.

For those still residing inside the country, the threat of raids and seizure of equipment is ever-present. Russia is currently among the top five countries (https://mmdc.ru/blog/2023/12/14/rossiya-okazalas-na-chetvertom-meste-po-kolichestvu-zhurnalistov-za-reshetkoj/) in the world for arrests of journalists. In addition, the threat of physical violence for those located both inside and outside Russia is constant, with journalists and civil society figures regularly beaten (https://novayagazeta.eu/articles/2023/07/04/novaya-gazeta-reporter-elena-milashina-and-attorney-alexander-nemov-attacked-in-russias-chechnya-en-news), tortured (https://www.amnesty.org/en/latest/news/2022/09/russia-activist-allegedly-beaten-and-raped-for-reciting-anti-war-poem-online/), poisoned (https://meduza.io/en/feature/2023/08/15/the-most-likely-explanation), and imprisoned (https://www.cnn.com/2024/03/29/media/russia-journalists-arrested-evan-gershkovich/index.html). Prominent opposition voices (https://meduza.io/en/news/2024/02/16/russian-opposition-politician-alexey-navalny-has-died) have been killed, or have died in custody. Russia is known for its "highly aggressive (https://freedomhouse.org/report/transnational-repression/russia)" practice of transnational repression, which involves the targeting of dissidents, human rights defenders, and other civil society members living in exile/outside Russia through different methods including poisonings and killings.

Beyond these physical threats, civil society groups operating inside Russia, in exile, or other groups working on Russian issues face a wide range of digital threats. A large number of civil society groups and independent media organizations have moved into exile since the 2022 full-scale invasion of Ukraine by Russia (https://books.openedition.org/pressesmines/9128). Today, many organizations-in-exile operate in a geographically dispersed and decentralized manner, making them dependent on online communications. The critical dependence on technology combined with frequent resource constraints makes these groups exceptionally vulnerable to a wide range of digital threats.

Censorship

Communications and information in Russia are subject to an extensive censorship regime, impacting the ability of audiences within Russia to access information and blocking the flow of information out of Russia. These restrictions include direct censorship of websites (https://meduza.io/en/news/2023/09/07/russian-authorities-reportedly-blocked-more-than-885-000-websites-in-first-half-of-2023) and social media platforms (https://www.themoscowtimes.com/2023/07/07/russia-blocks-metas-twitter-competitor-app-lawmaker-a81773) and blocking on specific communications protocols such as VPNs (https://roskomsvoboda.org/ru/analysis/vpn-russia-2023-eng/). This blocking also hampers organizing and coordination between domestic and foreign civil society organizations. For example, a 2023 report (https://citizenlab.ca/2023/07/an-analysis-of-in-platform-censorship-on-russias-vkontakte/) from The Citizen Lab on the Russian social networking site VK discovered that the platform "blocked content posted by independent news organizations, as well as content related to Ukrainian and Belarusian issues, protests, and lesbian, gay, bisexual, transgender, intersex, and queer (LGBTIQ) content."

Threats & Harassment

Prominent critics of the regime, antiwar activists, and independent media regularly face extensive intimidation and harassment campaigns both in and outside of Russia. These campaigns may include highly targeted online threats (https://storage.googleapis.com/istories/stories/2023/09/19/pust-ne-spyat-spokoino-vashi-gnidi/index.html), backed by meticulous research into the personal details and surveillance of the target.

Indirect Censorship Through Malicious Reporting and Pressuring Tech Platforms

Prominent regime targets are often subjected to extensive and coordinated campaigns to report social media accounts and posts on platforms, like Instagram and Facebook, with the goal of triggering account suspensions and post deletions. For example, a prominent Russian researcher and antiwar activist who spoke with us counted 83 complaints against her Instagram account submitted in a single 11-hour period in July 2024. The Russian government has also reportedly applied pressure on companies like Apple and Google to delete opposition (https://www.washingtonpost.com/business/2021/09/17/navalny-google-apple-app-russia/) and VPN (https://www.reuters.com/technology/russia-says-apple-blocks-25-vpn-apps-russia-ifx-reports-2024-07-04/) apps, as well as civil society YouTube videos (https://www.accessnow.org/press-release/youtube-russia-stop-supressing-free-speech/).

Account Takeovers and Honeypots

Beyond the sophisticated social engineering described in this report, popular chat programs, such as Telegram, are regularly targeted with a range of tactics (https://www.wired.com/story/the-kremlin-has-entered-the-chat/) for account hijacking and takeovers.

The number of tactics to target accounts and private information are too numerous to list, and are constantly evolving. For example, the co-founder of a Russian NGO that assists imprisoned antiwar activists described to us a new attack technique which relies on a fake Telegram "Helpline bot" impersonating the project of a genuine non-governmental organization. Such a fake helpline could be easily used to gather account information and identifying details from at-risk activists inside Russia, potentially as a precursor to eliciting sensitive information or account takeovers.

8. Protect Yourself & Your Colleagues

We believe that COLDRIVER and other Russian-government backed threat actors will persist in targeting civil society. While large email platforms continue to track and seek to disrupt these operators, this case shows that attacks can still make it through their defenses and into inboxes.

Do you think **you have been targeted by COLDRIVER, COLDWASTREL or other kinds of personalized phishing?** We encourage you to contact Access Now's Digital Security Helpline (https://www.accessnow.org/help/) to seek assistance.

Do you think that COLDRIVER or similar governmental phishing groups **may target you in the future**? If so, we encourage you to review the steps below. However, these recommendations are not comprehensive, and there is **no substitute for seeking expert assistance** from competent professionals such as Access Now's Helpline.

The following recommendations have been prepared jointly by Access Now and The Citizen Lab:

Start with prevention

Use two-factor authentication, correctly: Experts agree that setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked.

However, hackers like COLDRIVER and COLDWASTREL may try to trick you into entering your second factor; we have seen attackers successfully compromise a victim who had enabled 2FA. People using SMS-messaging as their second factor are also at greater risk of having their codes stolen, if a bad actor takes over their phone account.

We recommend that people use more advanced 2FA options such as security keys or, if they are Gmail users, Google Passkeys. Here are three guides for increasing the level of security for your account:

- Get Google Passkeys (https://www.google.com/account/about/passkeys/) (Google)
- How to: Enable two-factor authenticatio (https://ssd.eff.org/module/how-enable-two-factor-authentication)n (Electronic Frontier Foundation)
- Set up multi factor authentication (https://securityplanner.consumerreports.org/tool/set-up-multifactor-authentication-mfa) (Consumer Reports)
- Use a security key (https://securityplanner.consumerreports.org/tool/use-a-security-key-for-strongest-mfa) (Consumer Reports)

Enroll in programs for high-risk users. Google and some other providers offer optional programs for people who, because of who they are or what they do, may face additional digital risks. These programs not only increase the security of your account, but also flag to companies that you may face more sophisticated attacks. Such programs include:

- Google Advanced Protection (https://landing.google.com/advancedprotection/)
- Microsoft Account Guard (https://accountguard.microsoft.com)

- Proton Sentinel (https://proton.me/support/proton-sentinel)

Received a message? Be a five second detective

- **Step one: check your inbox for the sender's email.** Ask yourself if you have received messages from this account before. COLDRIVER often uses lookalike emails to impersonate people known to the target either personally or professionally, so may see an email that appears to come from someone you know, writing about something you would expect them to write about. Even if you have received previous messages from the same email address, it is possible to "spoof" a familiar looking email address, so move on to the next step.

- **Step two: check with the sender over a different medium**. If you have any concerns or are at all suspicious, do not open any PDF attachment or click on any link sent in the email. Instead, check directly with the purported sender, via another service, to confirm whether or not they've reached out to you. If you don't already have direct contact with them, consider asking someone you trust to inquire on your behalf.
- **Step three: don't just click.** Always consult an expert before opening a document you are unsure about. If you want to view a document that you think is probably safe, but want to take care, open the file *within* your webmail. Google, Microsoft, and others open the files on their computers and display the contents to you. This protects you from malicious code embedded in a document. But it **will not prevent you from clicking on potentially malicious links inside the document.**
  - If you are viewing an attached document inside your webmail, you should remain careful. **Don't just click on any links**; copy and paste them into your browser before visiting. Examine the domain carefully: Is it what you would expect for the site you expect to be visiting? Advanced phishing kits are very good at impersonating popular services, and often the only visual clue that it is not the authentic site will be in the address bar of the browser.
  - If you see a "login page" pop up, **stop**. This is a good time to consult a trusted expert.

- **Step four: beware of "encrypted" or "protected" PDFs.** This kind of message is almost always a cause for concern. Legitimately encrypted PDFs almost never include a single "click here" button inside the PDF, and they don't show a blurred version of the contents. Never click on any "login" links or "buttons" inside a PDF you have been sent.

Considering Online Virus Checking Sites? You may wish to use online virus scanning sites such as VirusTotal (https://www.virustotal.com/) or Hybrid Analysis (https://www.hybrid-analysis.com/) to check suspicious links or files.

- These services offer a useful service and can be part of a good security practice, but they come with a very important caveat: **when you use such free services, you are not the customer, you are the product.** Your files are available to many researchers, companies, and governments.
- We do not recommend using such tools to check "sensitive" files that may contain personal information or other private topics. Instead, contact a trusted expert that can help.

Think you are being targeted?

These recommendations address the kind of phishing that COLDRIVER and COLDWASTREL are currently using, but there are many other ways you could be targeted Whatever your level of risk, we encourage you to get personalized security recommendations from the Security Planner (https://securityplanner.consumerreports.org/), which also maintains a list of emergency resources (https://securityplanner.consumerreports.org/tool/emergency-resources/) and advanced security guides (https://securityplanner.consumerreports.org/tool/more-anonymity-security-help).

If you suspect that you have already been targeted in an attack, reach out to a trusted practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as partners, participants, grantees, and others. If this is the case, keep them informed about what has happened, what has been leaked, how this may impact them, and what steps you are taking to mitigate this impact.

If you believe you have been compromised: Access Now's Digital Security Helpline (https://www.accessnow.org/help/) is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in nine languages, including Russian (https://www.accessnow.org/help-ru/?ignorelocale).

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts, too. Consider using a password manager (https://securityplanner.consumerreports.org/tool/get-a-password-manager) to keep track of multiple passwords.
- You can also review access logs on your accounts, such as Proton Mail's Authentication Logs (https://proton.me/support/authentication-logs), Gmail's Last Account Activity (https://support.google.com/mail/answer/45938?hl=en), and review devices with account access (https://support.google.com/accounts/answer/3067630?hl=en), as well as Microsoft's Check recent sign-in activity (https://support.microsoft.com/en-us/account-billing/check-the-recent-sign-in-activity-for-your-microsoft-account-5b3cfb8e-70b3-2bd6-9a56-a50177863357). Some users may still have questions after reviewing these logs. We encourage you to make a copy of the logs if you suspect you may have been targeted, to share with an expert for review.

Acknowledgments

The Citizen Lab would like to express our deepest gratitude to the many targets and organizations with suspect messages that consented to share indicators and materials with us, and discuss their experiences. Without their participation, this investigation would have been impossible.

We would also like to thank many researchers and threat intelligence teams for feedback, including the teams at Mandiant, Microsoft Threat Intelligence Center, Proofpoint, and PwC.

We also thank Friendly Robot and TNG.

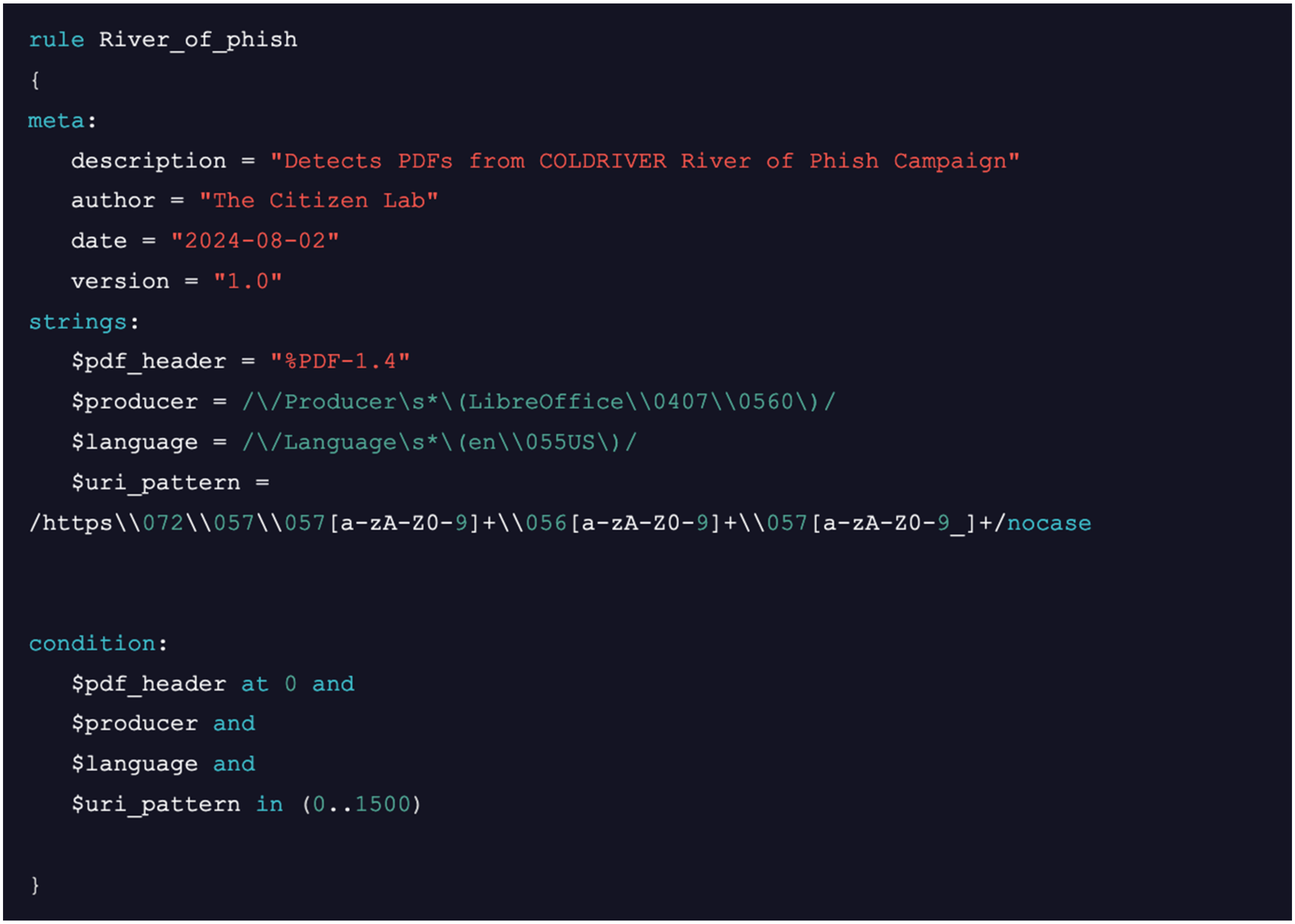
Thanks to our colleagues at The Citizen Lab Siena Anstis, Jakub Dalek, Bill Marczak, and Adam Senft for their careful review and editorial assistance, Mari Zhou for graphical assistance and report art, and Snigdha Basu and Alyson Bruce for communications support.

Appendix: Indicators of Compromise

COLDRIVER PDF Hashes

```
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d
0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88
efa2fd8f8808164d6986aedd6c8b45bb83edd70ca4e80d7ff563a3fbc05eab89
c1fa7cd73a14946fc760a54ebd0c853fab24a080cbf6b8460a949f28801e16fc
603221a64f2843674ad968970365f182c228b7219b32ab3777c265804ef67b0a
df9d77f3e608c92ef899e5acd1d65d87ce2fdb9aab63bbf58e63e6fd6c768ac3
384d3027d92c13da55ceef9a375e8887d908fd54013f49167946e1791730ba22
79f93e57ad6be28aae62d14135140289f09f86d3a093551bd234adc0021bb827
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e
```

Yara Rule for River of Phish PDFs



```
rule River_of_phish
{
meta:
   description = "Detects PDFs from COLDRIVER River of Phish Campaign"
   author = "The Citizen Lab"
   date = "2024-08-02"
   version = "1.0"
strings:
   $pdf_header = "%PDF-1.4"
   $producer = /\/Producer\s*\(LibreOffice\\0407\\0560\)/
   $language = /\/Language\s*\(en\\055US\)/
   $uri_pattern =
/https\\072\\057\\057[a-zA-Z0-9]+\\056[a-zA-Z0-9]+\\057[a-zA-Z0-9_]+/nocase


condition:
   $pdf_header at 0 and
   $producer and
   $language and
   $uri_pattern in (0..1500)

}
```

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2024/08/Yara-rule-for-river-phish-1.png&nocache=1)

COLDRIVER First-stage Domains

ithostprotocol[.]com
xsltweemat[.]org
egenre[.]net
esestacey[.]net
ideaspire[.]net
eilatocare[.]com
vocabpaper[.]com
matalangit[.]org
togochecklist[.]com

COLDWASTREL PDF on VirusTotal

4a9a2c2926b7b8e388984d38cb9e259fb4060cccc2d291c7910be030ae5301a3

COLDWASTREL Domains

protondrive[.]online
protondrive[.]services (tentative)
protondrive[.]me (tentative)
service-proton[.]me (Per Access Now's analysis)

Privacy Policy (https://citizenlab.ca/privacy/)

(http://munkschool.utoronto.ca/)

EXHIBIT 6

Phishing Attacks Targeting Ukrainian NGOs for AccessNow

For 7 years, Digital Security Lab Ukraine has been providing security support to the civil society sector in Ukraine. Thanks to our long-standing work, we have had the opportunity to observe changes in this field, document security incidents, and conduct risk assessments together with our beneficiaries and partners.

Among the common risks, our beneficiaries rate account hacking as the highest risk. They consider device compromise to be significantly less likely. However, it's important to note that risk assessment largely depends on the organization's activities, its products or results, and the broader context. When detailing the risks, we see that the greatest concern is caused by phishing-based account compromises and device compromise through the installation of malicious software.

From our side, as we document security events (incidents), we observe regular waves of targeted phishing campaigns and consistently high levels of mass commercial phishing.

Regarding the assets most frequently targeted by phishing attacks, these are services commonly used by representatives of the Ukrainian civil society sector. Among the most popular are Google, Microsoft, Ukr.net, Facebook, Instagram, Telegram, X (Twitter), WhatsApp, and Signal. The largest share of successful phishing attacks targets online accounts, where attackers impersonate legitimate customer support representatives. In particular, since 2022, due to Ukrainians actively highlighting the consequences of Russian aggression, social media platforms have increased often unjustified content or account blockings (Facebook, Instagram). This trend is exploited by attackers in their phishing campaigns, impersonating platform support teams and threatening to block accounts. You can find examples of such campaigns at this or this link.

Similar tactics are used by attackers in phishing through popular messengers. From 2022 to 2024, we've seen the highest number of such cases in Telegram. Attackers impersonate Telegram support, intimidate users by claiming that someone has gained access to their account, and ask them to verify their account ownership. This way, they obtain the SMS code, two-factor authentication password, or prompt users to add a new session. Another common scheme involves using bots that imitate official sources of information about current events, such as power outages. In the case of Telegram, the situation is further complicated by the company's lack of communication with users and failure to respond to malicious activities.

There is growing concern about phishing in messengers and services that are positioned as "secure" (using end-to-end encryption). In Proton, Signal, and WhatsApp, attackers exploit several beliefs at once. First, the idea that people tend to trust more in "secure" services and may react less cautiously to phishing messages. Second, the use of political context. In Ukraine, petition services are a popular way of influencing the government, so attackers create phishing messages and websites exploiting these services. We’ve described this scheme in more detail in this publication.

In account hacking attempts, it is often difficult for us to attribute the attack due to a lack of technical, human, financial, or other resources, or the inability to gather indicators. However, in the case of phishing attacks with malicious attachments, they contain significantly more indicators. We can obtain the original message, analyze IOCs and TTPs, and compare them with known past incidents or reports. Over the years, we have observed waves of targeted phishing attacks using malicious attachments. These are usually associated with hacker groups sponsored by Russia, and less frequently with financially motivated attacks. Attackers attempt to impersonate official government agencies, such as the Security Service of Ukraine (SBU), courts, tax authorities, military structures, and others.

The most common goal of such phishing is espionage, and less frequently, the destruction or restriction of access to data. In such cases, phishing may serve as the initial stage for more complex tasks (initial access). Malicious software most often targets Windows OS, although there have been cases involving Android OS. Among the actors most often attributed, we have seen Gamaredon (Primitive Bear, Tridentursa), but we do not have enough data for statistical analysis.

EXHIBIT 7

FILED UNDER SEAL

EXHIBIT 8

FILED UNDER SEAL

EXHIBIT 9

FILED UNDER SEAL

EXHIBIT 10

FILED UNDER SEAL