citizenlab.ca /2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

Rivers of Phish Sophisticated Phishing Targets Russia's Perceived Enemies Around the Globe

John Scott-Railton, Rebekah Brown, Ksenia Ermoshina, Ron Deibert ⋮⋮ 8/14/2024

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, Arjuna Team, and 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 to read the Access Now Report and the Access Now Helpline Technical Brief.

1. River of Phish: Campaign Overview

Our collaborative investigation with Access Now, with the assistance of multiple additional civil society organizations including First Department, Arjuna Team, and 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 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 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.

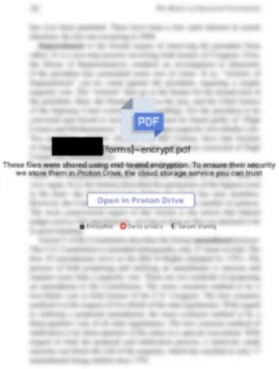
Importantly, we suspect that the total pool of targets is likely much larger than the civil society groups whose cases we have analyzed. We have observed US government personnel impersonated as part of this campaign, and given prior reporting about COLDRIVER's targeting, we expect the US government remains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

Open in Proton Drive

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 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) 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. 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 or another phishing platform. We note that COLDRIVER has been observed using Evilginx in recent cases.

Our investigative partner, Access Now, has included a description of the fingerprinting code in their Technical Brief. The fingerprinting code was obfuscated using the Hunter PHP Javascript Obfuscator, a tool that is publicly available on GitHub.

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 or this one 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	Language
b07d54a178726ffb9f2d5a38e64116cbdc361a1a0248fb89300275986dc5b69d	Gracelyn Reilly	LibreOffice 7.0	en-US
0ded441749c5391234a59d712c9d8375955ebd3d4d5848837b8211c6b27a4e88	Talon Blackburn	LibreOffice 7.0	en-US
efa2fd8f8808164d6986aedd6c8b45bb83edd70ca4e80d7ff563a3fbc05eab89	Howard Howe	LibreOffice 7.0	en-US
384d3027d92c13da55ceef9a375e8887d908fd54013f49167946e1791730ba22	Annabelle Kline	LibreOffice 7.0	en-US
00664f72386b256d74176aacbe6d1d6f6dd515dd4b2fcb955f5e0f6f92fa078e	Paulina Mullen	LibreOffice 7.0	en-US
79f93e57ad6be28aae62d14135140289f09f86d3a093551bd234adc0021bb827	Emery Hogan	LibreOffice 7.0	en-US

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, for example).

In January of 2024, Google’s Threat Analysis Group (TAG) reported 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). 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 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 governments 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 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 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
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, which they track as *Star Blizzard* (previously *SEABORGIUM*). Google's Threat Assessment Group (TAG) reported on them as *COLDRIVER*, PWC reported on them as *Blue Callisto,* Proofpoint reported on them as TA446, Sekoia reported 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."

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 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.

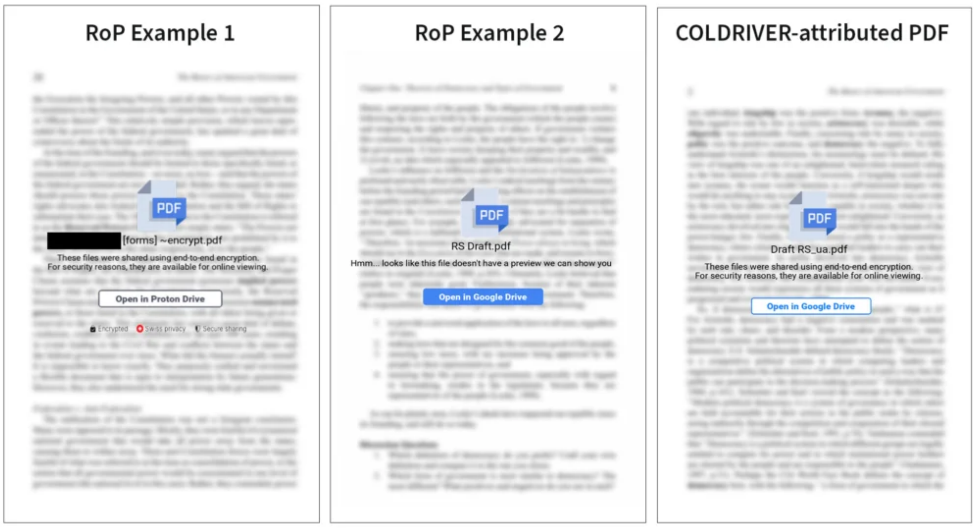
Like the River of Phish ("RoP") PDFs (See: Table 2 above), those shared by Proofpoint included identical LibreOffice versions, seemingly-randomized author names, and en-US language settings.

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

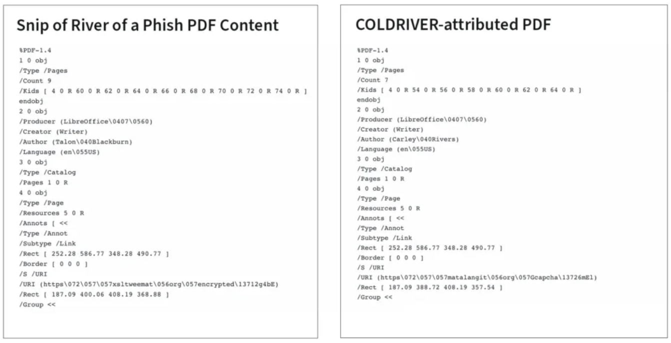
Hmm... looks like this file doesn't have a preview we can show you

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.

Figure 2: Two River of Phish PDFs and one COLDRIVER PDF (Note: The Example 1 screenshot has been redacted to remove the nar



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 <<
```

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
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).

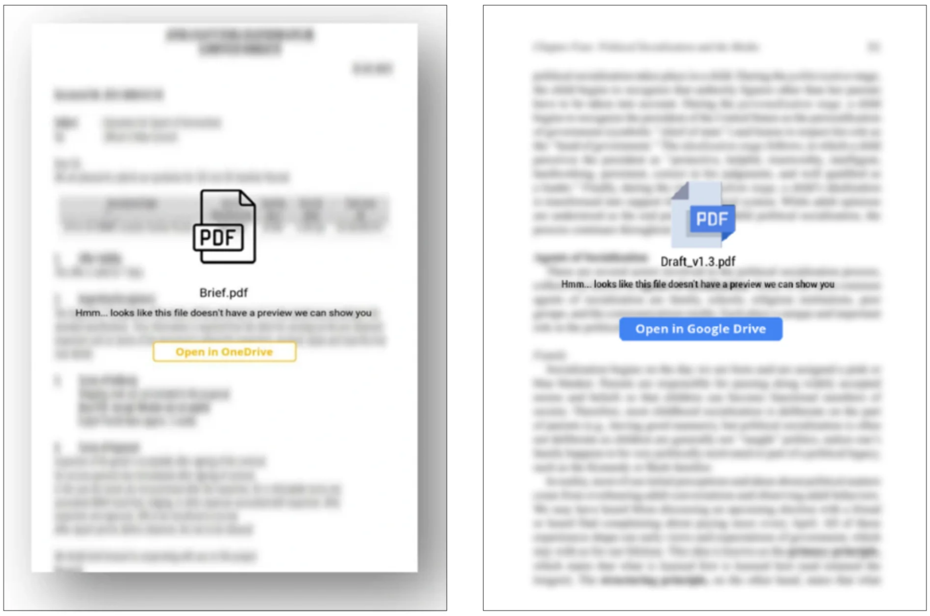

PDF
Brief.pdf
Hmm... looks like this file doesn't have a preview we can show you
Open in OneDrive
PDF
Draft_v1.3.pdf
Hmm... looks like this file doesn't have a preview we can show you
Open in Google Drive

Figure 4: PDF sent in a campaign reported by Microsoft in December 2023 (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 the practice of embedding HubSpot domains in the targeting PDF in an attempt to evade detection.

River of Phish: Signs of Continued Evolution?

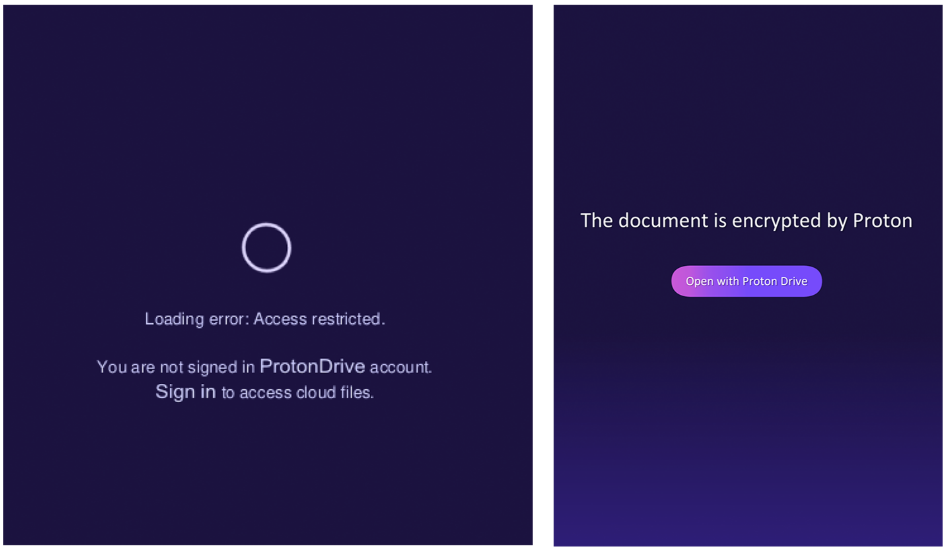
In addition to the previous use of HubSpot, earlier COLDRIVER reporting mentioned clusters of domains named around a particular theme or service being impersonated, such as *proton-docs[.]com*, *proton-reader[.]com*, and *proton-viewer[.]com* reported by Microsoft in 2022. However both Microsoft and Recorded Future noted that COLDRIVER appeared to be using a "more randomized" 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 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

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 multiple targets
Links in PDF	Redirected to fingerprint, then to separate domain/site to gather credentials	Hosted the phishing kit directly.

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

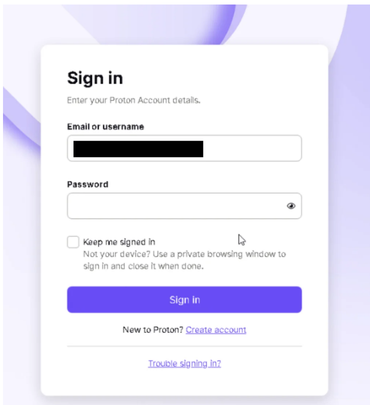
In addition to the differences in the PDF content and metadata, there were several other notable differences between the two attacks:

- 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. 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.

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, 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 of espionage that reaches back to pre-Soviet times, and has engaged in cyber espionage campaigns and active cyber operations for decades. These operations have been extensively studied by academics, civil society organizations, journalists, governments and the commercial cybersecurity community. Generally, Russian cyber espionage and active cyber operations are undertaken independently by multiple (and sometimes competing) state security agencies, occasionally with the participation of organized criminal groups or other private sector entities (e.g., NTC Vulkan, RomCom, Cadet Blizzard).

There are several Russian and Russian-aligned entities that undertake or are responsible for cyber espionage (see here). 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 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 operations designated as APT28, Fancy Bear, and Sandworm, and has been linked to DDoS and disruptive malware attacks on critical infrastructure, the financial sector, government and non-governmental organizations, and other sectors. The US, UK and other Western governments have also linked 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, 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 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 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 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 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, which has been growing in scope and scale worldwide.

In 2017, for example, The Citizen Lab published a report 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 firms, have formally acknowledged 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 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 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, tortured, poisoned, and imprisoned. Prominent opposition voices have been killed, or have died in custody. Russia is known for its "highly aggressive" 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. 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 and social media platforms and blocking on specific communications protocols such as VPNs. This blocking also hampers organizing and coordination between domestic and foreign civil society organizations. For example, a 2023 report 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, 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 and VPN apps, as well as civil society YouTube videos.

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 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 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:

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:

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 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.

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)

}
```

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)