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.

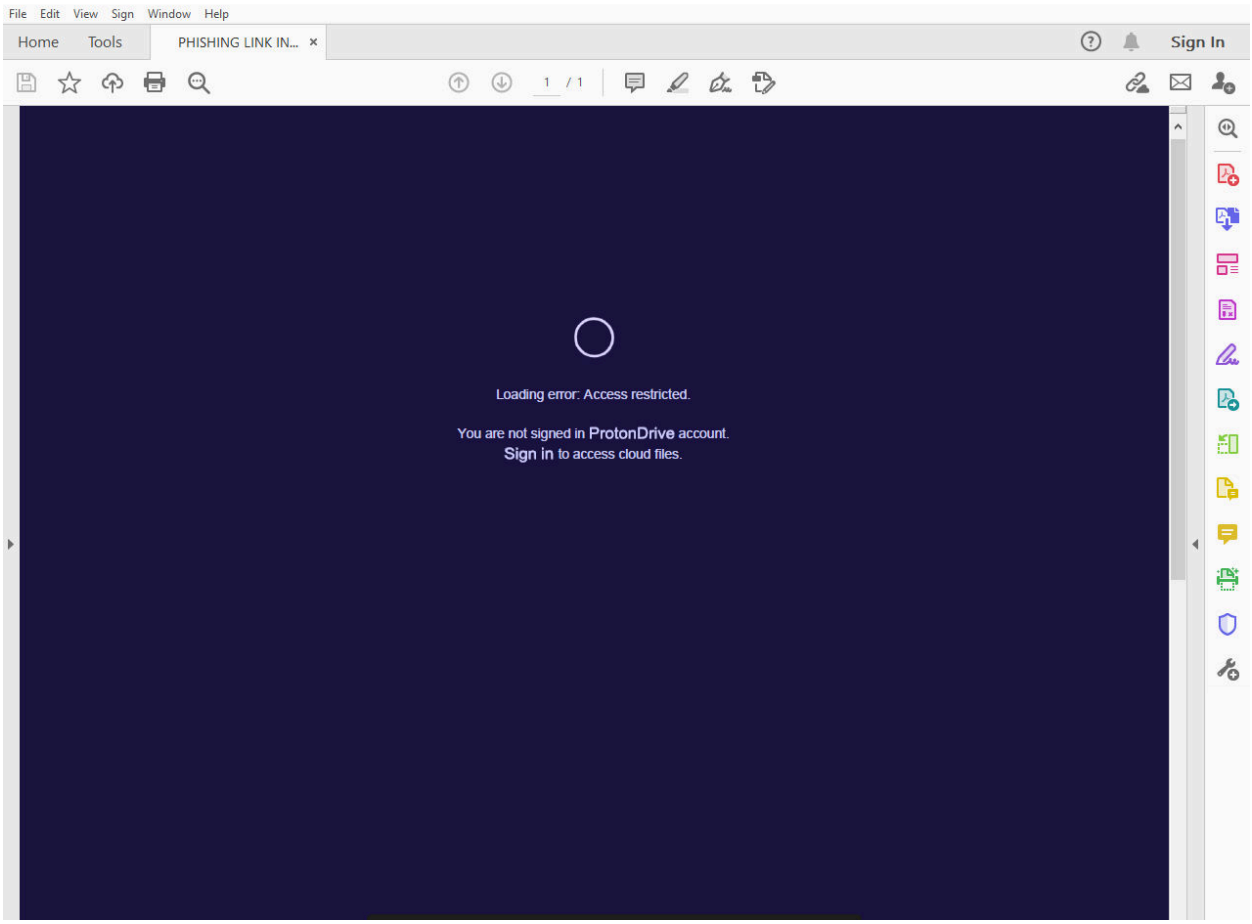
Here's an example, using a pseudonym:

> 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.

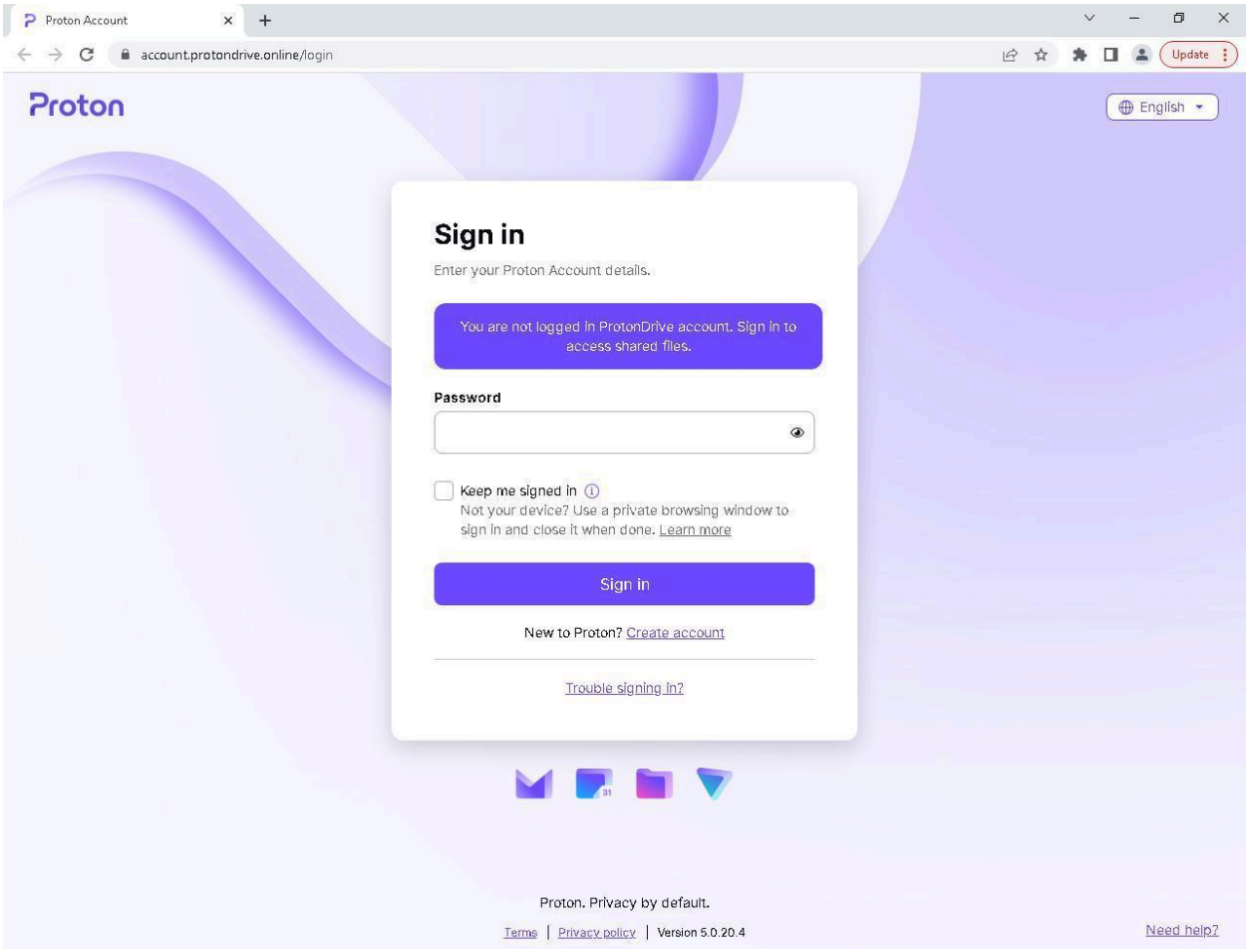
In some of the cases analyzed, the emails contained a PDF attachment which appeared to be locked. The same emails provided a link that purported to help unlock the PDF (see screenshot below).



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):



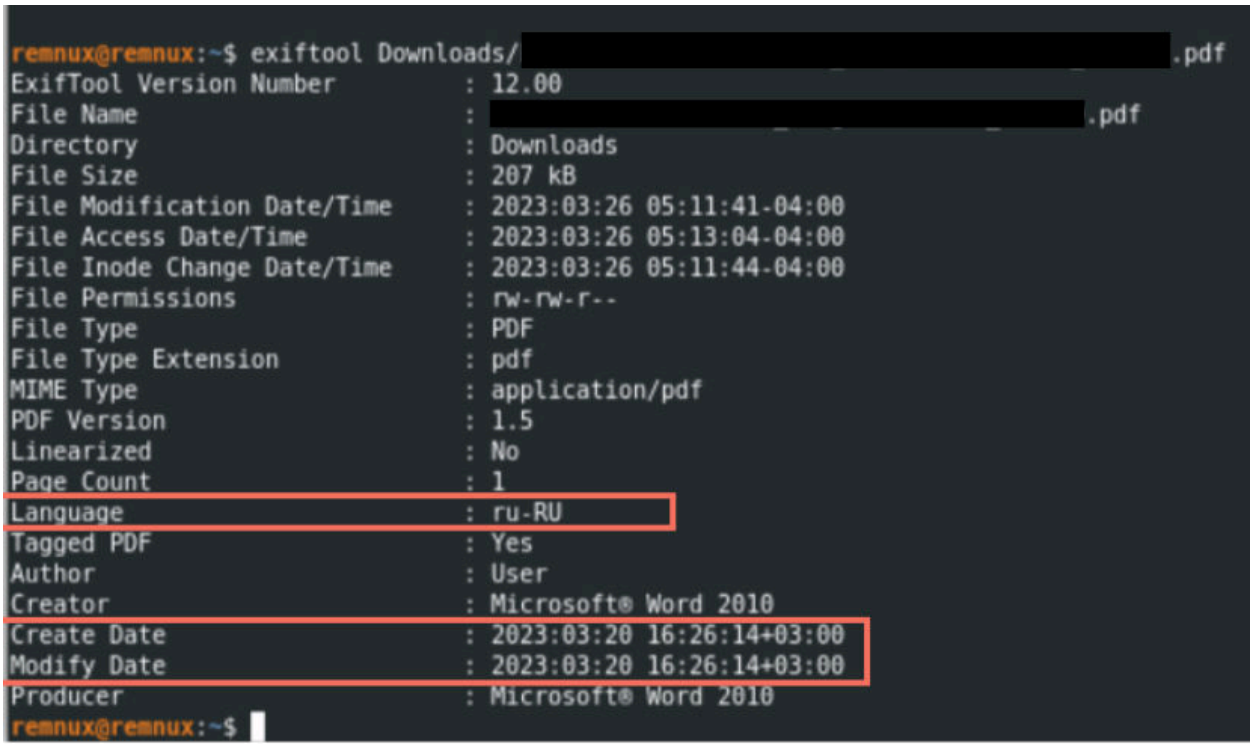
Sample of fake Proton Mail login page presented to targets as part of COLDWASTREL campaign.

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.



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.

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:

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