COLDWASTREL of space

By John Southworth, PwC Threat Intelligence

Further infrastructure analysed for COLDWASTREL/White Dev 185 campaigns targeting NGOs.

On 14th August 2024, The Citizen Lab and AccessNow released reports on two threat actors: COLDRIVER (which we track as Blue Callisto) and COLDWASTREL (which we track as White Dev 185).[1] [2] PwC was referenced for previous work on Blue Callisto,[3] but we focus our analysis on White Dev 185 in this blog.

Through analysing the infrastructure that The Citizen Lab and AccessNow attribute to COLDWASTREL, we observed the following default webpage response (with SHA-256: fe563fa9ba8a8a70ef622a403228404910fdf4dd06ab3f154ec5009e5edb5e98) used on domains, for example on account[.]protondrive[.]online.

```
<head>
    <title>The page is temporarily unavailable</title>
</head><body>


</body>
```

Looking for further infrastructure returning this response, we observed 24 unique domains used between 2021 and 2024 which we assess are highly likely related to White Dev 185:

- accounts-proton[.]me
- center-facebook[.]com
- desktop-facebook[.]com
- drive-proton[.]com
- email-pm[.]me
- link-pm[.]me

- livecloudaccount[.]com
- online-facebook[.]com
- onlinestorageroute[.]space
- open-button[.]com
- proton-drive[.]me
- proton-service[.]services
- proton-verify[.]me
- protondrive[.]online
- protondrive[.]services
- secure-pm[.]me
- security-gm[.]com
- service-pm[.]me
- service-proton[.]com
- service-proton[.]me
- services-proton[.]me
- support-gm[.]com
- support-ukr[.]net
- verify-proton[.]me

Approximately half of these domains use ‘Proton’ as a theme, but other themes such as Facebook or generic cloud/email services are also used, as well as abbreviated references to particular countries (i.e. 'support-ukr[.]net' is likely referencing Ukraine).

Based on the observed domains, we performed pDNS pivots to also link the following IP addresses to White Dev 185:

IP address	Year used	Country geolocation	Hosting provider
45.138.87[.]108	2024	Romania	EstNOC OY
185.227.68[.]188	2024	Finland	EstNOC OY
45.146.222[.]32	2024	Serbia	EstNOC OY
45.133.195[.]117	2024	Norway	EstNOC OY
46.246.1[.]187	2024	Sweden	EstNOC OY
185.227.68[.]179	2024	Finland	EstNOC OY
185.195.236[.]68	2024	Hungary	EstNOC OY

38.180.18[.]66	2024	Belgium	M247 Europe SRL
185.247.224[.]39	2023	Romania	FlokiNET ehf
185.165.169[.]238	2023	Iceland	FlokiNET ehf
5.252.178[.]137	2023	Romania	MivoCloud SRL
194.180.174[.]66	2023	Moldova	MivoCloud SRL
91.196.68[.]11	2023	Germany	EstNOC OY
45.129.33[.]34	2023	Czech Republic	EstNOC OY
45.128.134[.]140	2022	France	EstNOC OY
185.225.17[.]26	2022	Romania	MivoCloud SRL
194.36.189[.]125	2022	Netherlands	Host Sailor Ltd
46.166.176[.]207	2021	Netherlands	NForce Entertainment B.V.
195.54.163[.]207	2021	Ukraine	Green Floid LLC
185.106.123[.]111	2021	Netherlands	Host Sailor Ltd
5.181.156[.]67	2021	Moldova	MivoCloud SRL
194.180.174[.]176	2021	Moldova	MivoCloud SRL
46.166.176[.]205	2020	Netherlands	NForce Entertainment B.V.
185.198.57[.]213	2020	Netherlands	Host Sailor Ltd
87.120.8[.]80	2020	Bulgaria	Neterra Ltd.

We note that not all of these IP addresses are likely controlled by White Dev 185 any longer, but include them as IoCs for historical hunting purposes. We also note several patterns of preferred hosting providers, mainly favouring ‘EstNOC OY’ from 2022 onwards, and that the infrastructure used also pushes back White Dev 185/COLDWASTREL’s initial activity to 2020.

Based on these IP addresses, we performed some further pDNS pivots for other infrastructure in the respective timeframes for each IP. We include all infrastructure results as indicators at the end of the blog.

Further threat actor links

Based on the use of the domain support-ukr[.]net, and the general approach of the campaigns (using spear phishing with PDF attachments for credential stealing), we assess with realistic probability that the campaigns CERT-UA track under the name UAC-0102 are related to White Dev 185.[4]

Further, based on this domain support-ukr[.]net, we observed that it resolved to 185.106.123[.]111 in 2021. This IP address also had the following domain resolutions in the same timeframe:

- mail-ukr[.]net
- email-ukr[.]net

The domain mail-ukr[.]net had been attributed by Microsoft in 2015 to what it previously called STRONTIUM,[5] now tracked as Forest Blizzard (a.k.a. APT28, BlueDelta, Fancy Bear), which we track as Blue Athena. We also previously attributed email-ukr[.]net to Blue Athena in 2016.

Given the time difference between the initial use of these domains (2015/16) and them beginning to resolve again in 2021 along with differences in WHOIS registration information between the two time periods, we treat this as a low confidence pivot, as it could also be explained by the domain being reused

by a separate threat actor six years later. The IP address that both domains resolved to (185.106.123[.]111) fits the pattern of being highly likely White Dev 185 (given hosting provider ‘Host Sailor Ltd’, which has been used previously by the threat actor, and having previously been resolved to by support-ukr[.]net), so we assess it is unlikely that this is some kind of sinkhole. As such, the two main hypotheses we assess are possible are:

- mail-ukr[.]net and email-ukr[.]net were previously both used by Blue Athena in 2015/16, and then reused by a separate threat actor (White Dev 185) in 2021; or
- White Dev 185 is Blue Athena.

Given this single attribution point, we do not have enough evidence at this stage to rule out either hypothesis. As such, for now, we assess that White Dev 185 is related to Blue Athena with a realistic probability, with low confidence.

Indicators of compromise

Indicator	Type
account-api[.]cloudstorageservice[.]online	Domain
account-api[.]onlinestorageroute[.]space	Domain
account-api[.]protondrive[.]online	Domain
account[.]email-pm[.]me	Domain
account[.]onlinestorageroute[.]space	Domain
account[.]open-button[.]com	Domain
account[.]proton-drive[.]me	Domain
account[.]proton-service[.]services	Domain
account[.]proton-verify[.]me	Domain
account[.]protondrive[.]online	Domain
account[.]protondrive[.]onlinestorageroute[.]space	Domain
account[.]protondrive[.]services	Domain
account[.]secure-pm[.]me	Domain
account[.]service-pm[.]me	Domain
account[.]service-proton[.]com	Domain
account[.]service-proton[.]me	Domain
account[.]services-proton[.]me	Domain
accounts-proton[.]me	Domain
accounts[.]support-ukr[.]net	Domain
center-facebook[.]com	Domain
civic-synergy[.]online	Domain
cloudstorageservice[.]online	Domain
desktop-facebook[.]com	Domain
drive-proton[.]com	Domain
drive[.]link-pm[.]me	Domain
drive[.]proton-verify[.]me	Domain
drive[.]secure-pm[.]me	Domain
drive[.]service-pm[.]me	Domain
drive[.]service-proton[.]me	Domain

edisk[.]support-ukr[.]net	Domain
email-pm[.]me	Domain
email-ukr[.]net	Domain
email[.]support-ukr[.]net	Domain
en-us[.]center-facebook[.]com	Domain
en-us[.]desktop-facebook[.]com	Domain
fb-me[.]com	Domain
fidh[.]tech	Domain
fr-fr[.]center-facebook[.]com	Domain
h[.]maiils[.]com	Domain
link-pm[.]me	Domain
livecloudaccount[.]com	Domain
login[.]livecloudaccount[.]com	Domain
login[.]security-gm[.]com	Domain
login[.]support-gm[.]com	Domain
m[.]h[.]maiils[.]com	Domain
maiils[.]com	Domain
mail-api[.]onlinestorageroute[.]space	Domain
mail-api[.]protondrive[.]online	Domain
mail-ukr[.]net	Domain
mail[.]civic-synergy[.]online	Domain
mail[.]fidh[.]tech	Domain
mail[.]onetimeopportunity[.]store	Domain
mail[.]onlinestorageroute[.]space	Domain
mail[.]protondrive[.]online	Domain
mail[.]support-ukr[.]net	Domain
n[.]maiils[.]com	Domain
na[.]maiils[.]com	Domain
old[.]onlinestorageroute[.]space	Domain
old[.]protondrive[.]online	Domain
online-facebook[.]com	Domain
onlinestorageroute[.]space	Domain
open-button[.]com	Domain
oui6473rf[.]xxuz[.]com	Domain
proton-drive[.]me	Domain
proton-service[.]services	Domain
proton-verify[.]me	Domain
protondrive[.]online	Domain
protondrive[.]services	Domain
reports[.]onlinestorageroute[.]space	Domain
reports[.]protondrive[.]online	Domain
ru-ru[.]center-facebook[.]com	Domain
ru-ru[.]desktop-facebook[.]com	Domain
secure-pm[.]me	Domain
secure[.]onlinestorageroute[.]space	Domain
secure[.]protondrive[.]online	Domain

security-gm[.]com	Domain
service-pm[.]me	Domain
service-proton[.]com	Domain
service-proton[.]me	Domain
service[.]link-pm[.]me	Domain
services-proton[.]me	Domain
support-gm[.]com	Domain
support-ukr[.]net	Domain
verify-proton[.]me	Domain
verify-proton[.]me	Domain
view-menu[.]site	Domain
webmail[.]civic-synergy[.]online	Domain
45.138.87[.]108	IPv4 Address
194.180.174[.]66	IPv4 Address
185.227.68[.]188	IPv4 Address
91.196.68[.]11	IPv4 Address
45.133.195[.]117	IPv4 Address
87.120.8[.]80	IPv4 Address
45.146.222[.]32	IPv4 Address
38.180.18[.]66	IPv4 Address
185.198.57[.]213	IPv4 Address
46.246.1[.]187	IPv4 Address
45.128.134[.]140	IPv4 Address
185.227.68[.]179	IPv4 Address
185.247.224[.]39	IPv4 Address
46.166.176[.]205	IPv4 Address
195.54.163[.]207	IPv4 Address
45.129.33[.]34	IPv4 Address
185.106.123[.]111	IPv4 Address
5.252.178[.]137	IPv4 Address
185.165.169[.]238	IPv4 Address
5.181.156[.]67	IPv4 Address
185.195.236[.]68	IPv4 Address
46.166.176[.]207	IPv4 Address
185.225.17[.]26	IPv4 Address
194.180.174[.]176	IPv4 Address
194.36.189[.]125	IPv4 Address

---

[1] ‘Rivers of Phish: Sophisticated Phishing Targets Russia’s Perceived Enemies Around the Globe’, The Citizen Lab, https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/ (14th August 2024)

[2] ‘Spear-phishing cases from Eastern Europe in 2022-2023 and 2024: a technical brief’, AccessNow, August 2024, https://www.accessnow.org/wp-content/uploads/2024/08/Spear-phishing-cases-from-Eastern-Europe-in-2022-2024-a-technical-brief.pdf

[3] ‘Blue Callisto orbits around US Laboratories in 2022’, PwC, https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html

[4] ‘Targeted UAC-0102 cyber attacks against UKR.NET service users (CERT-UA#6858)’, CERT-UA, https://csirt.csi.cip.gov.ua/en/posts/uac-0102-cyber-attacks (2nd August 2023)

[5] ‘Microsoft Security Intelligence Report: Volume 19’, Microsoft, June 2015, https://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf