

CERT-UA

Archived: 2026-04-06 00:24:22 UTC

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 42b6b2533135574ac8a2027df465b295 4d6eac0b0dd1adc47d81b163d03e5f4b a03cb9a28fa5ce72354e1556731a68d4 4d549fa15eadeefd30f5269a2b3995c4 7ffb80d87ab0fe5e2c7f7338ec22a7b0 ed7bb4cc6dd1079efbe4bc3ceffd4250 9997462826c26ab82a29e1c0712bbbb5 6fe2a60e3f4c15c60128562d006696b6	b10bc0bb30b3c1d0c404d3a902ccebca425f23cb5a66c02104739f226c77b5816 05457a790782542d3f16c9b8368a077b458ff7349856e6da541223a51e94b9c8 91e9325dd4972c0d40becfff6e65399c46aeb210a3b9a1f75d453cc8fe87d09c cf919033a2a4f76a4b78499be027090a0a7980a2f536df53eebb2140478abeb7 521c8345351144437033b41dfb5e4878c3b3a7ade4e2d0ccdcc5699d0b4d3ac6 3442724f36fcaa1822bdafc3417e6bc7488898c4acbc73f0114ffeb6a3604164 d8236c841b07c933d4de0ef9ed854902f6aae73b83137d9ffbe29fb879aa094f 2708b9f8a196c50c8c6d6001af5b02e3c5d113e1977a686319eae7652ecbc1d3 72028cff34d33e26bf01e4bf63c8b977ece33b3809bd6dd075bcfff343895dc4b
--	--

Host-based:

```
%APPDATA%\XmlSchemaMicrosoftXsd.xml
%APPDATA%\XmlSchemaMicrosoftXsd0.xml
%PUBLIC%\MicrosoftUpdateClient\
%PUBLIC%\MicrosoftUpdateClient\Microsoft_update_tool_%NUM%.dat
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe' -argumentlist ""`$a=whoami;"
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe' -argumentlist ""`$a=whoami;"
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%/59948e7126a2927a53af0593f85dad2f5ae5c6e0.ph
hXXps://troadsecow[.]com/gkaslnwqpasg/usersfolders/%SID%/62d4677fcf60ac0c4933bd80dec255868827e00.ph
hXXps://troadsecow[.]com/gkaslnwqpasg/usersfolders/%SID%/9f5fe4bab163de5eedb995beed21c75578284fa4.ph
hXXps://troadsecow[.]com/lg5362s5215098-xvbxzcnasaf4lmsa.php
hXXps://troadsecow[.]com/lg5362s5215098-xvbxzcnasaf4lmsa.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

