CERT-UA

Archived: 2026-04-05 14:40:26 UTC

Загальна інформація

Фахівцями Trendmicro 22.12.2023 поінформовано CERT-UA про виявлення підозрілих файлів більшість з яких стосувалася тематики війни.

На основі отриманої інформації CERT-UA вжито заходів з дослідження серії кібератак які, під виглядом рекрутингу до 3-тьої окремої штурмової бригади та Армії оборони Ізраїлю (ЦАХАЛ), проводяться проти військовослужбовців Збройних Сил України.

З'ясовано, що не пізніше листопада 2023 року невстановленими особами засобами Signal здійснюється розповсюдження архівів, що містять LNK-файли, запуск яких ініціює ланцюг ураження шкідливими програмами REMCOSRAT і REVERSESSH, що призведе до створення технічних умов несанкціонованого віддаленого доступу до ЕОМ для зловмисників.

Як правило, згадані файли-ярлики містять обфусковану команду для завантаження і запуску за допомогою mshta.exe HTA-файлу, в якому знаходиться обфускований програмний код. В свою чергу VBScript-код здійснить запуск PowerShell-команди, що призначена для розшифрування (AES-128-ECB), декомпресії (GZIP) та запуску PowerShell-сценарію. Останній забезпечить завантаження і запуск файлу(-ів) шкідливої програми, а також документ-приманку (PDF або DOCX). При цьому, назви та вміст таких документів є також дуже релевантними для військових: "опитування полоненого", "геолокації", "команди кодування", "позивні" тощо.

Зауважимо, що, незважаючи на використання публічно доступного інструментарію (що може призводити до виявлення схожостей з іншими атаками), описана активність за іншими специфічними ознаками є окремим кластером кіберзагроз та відстежується за ідентифікатором UAC-0184.

Нагадуємо, що у разі виявлення підозрілої активності на ЕОМ та в ІКС Збройних сил України просимо невідкладно інформувати Центр кібербезпеки ІТС (в/ч А0334; email: csoc@post.mil.gov.ua).

Індикатори кіберзагроз

Файли:

```
7164008af682b5f3567d50700b4a1b8b    4b36a82e1781ffa1936703971e2d94369e3059c8524d647613244c6f9a92690b
7c05cfed156f152139a6b1f0d48b5cc1    e4615b74d62f384d23e58bc467c615b17779e4f8084c8a0134db97a5e642027f
b1f8484ee01a7730938210ea6e851888    88f0722c907100ef09049c82032a0ac66afa153d03fb89d378ae65f6e5890a3f
0b3c248f579a8f5865972218e63c3b34    ef6edacf6ee1e0dd2e53046a91ba84d10a8adda6918ca7aac6e96ead432efbbc
f5ee6aa31c950dfe55972e50e02201d3    5fff1cd29bb6e6cfe9516b70f9f44755098392c2e2a0f4784486182c309b2c99
56154fedaa70a3e58b7262b7c344d30a    f650a9f1930e55e405d7121c56b90a996ab213a05b772a8f02ceb1cdbeb91165
7f87d36c989a11edf0de9af392891d89    c5452b859922b9633839e092f09f0ce4818b6085043360c90c0b0f2bfad9fca1
```

```
5c734bb1e41fab9c7b2dabd06e27bc7b  bd871a2ccd6d7c4f89f9f5087e60cfdcc7ab35b670cfda7ddfd6dbbab8c8560c
0e4f60ad19a3ed01cb68a9df24c0eef4  0bbef4f3682eb8f76c032aa0515ae122ad6f03a8bfe1303b87c6b92cd363e2bc
34d817cbc38256ebf8bd8cefe92a060e  55ddf9f5f5b517971298686ab4ac13e85bacea43ec79191d622308b08e059d6a
e3213e545d5169a30fa3e809ced0ab96  25dfb146058787af6b4c12be9b2ffa6479eb64d7f167adf51bf1ed9851cf0fca
10a54d8a77530ef910e36b5df50bd8e1  c00dd156d786bb607fe405059d628bbf0abaccc6b388031fe9b043e4c54cf264
e262dc9c87d6ae1063f402a9a10da4ee  fd9c5fe5a1729b7c796a9f53e1870742d35ab5559a8249fe73aed502ba4e14d7
af3044b499611683626805da55e3cdc5  ff2cfdedfb2e6ff63de97a00a23a9c1c07ac6f8529bca62bb97d871ace4f8a42
81048decf4476da7b2c0145433e0757a  3b80e140b995ca6eef2d3f56ac2df1efd6b7f45f5e79d4cbfbaf3aed4d0e7a96
fa998db4becc688ff36f827e1f3c941b  92a7a3c2b5c674d523226fa4937d25e0dd10817b4d64d5588b0282e2b73ce660
1278f00a2ce547241d3cad9f05b8228a  54b3fa9492289a7efa717e5fe0750084dea1b1d613cc91720f14665f2b4ad2d8
f412b0ba82b500448e7a52f5d4cf5541  15483f5352ba0971974c3fcf3154b64bc73b290aa64d3316409eda1917f8dc9a
876c77e91c119ccb922eec8155a3d113  46867d58775f609f5926d3532db7b9b8ed383df2817b1b338fc95b4e6791f84a
31f626793ee177f6029e2269f1ec8b16  2d95d3f5177df2ae075f6428568dfeaa669e79b9567a094491741cc2d12d9a24
aa92b76c20602e8becf16548d1c127b9  3a8a3ad0f520c49d5ade4ddfc6cf2542f38f44b6328efff6b6953cce3cac4007
a5cb89f4d786bbcfa701489bc2b9c6fc  579882c876ecb93ffcc692a0bd727f0ee5e9a48baae8add8c08d3ee6e479ed2a
415673c482768861b7d1dcbfaff74010  c4ce4e9e65c7d728ff835ad658463d05d94b1e7ee3e223aed08d6094123e1b9b
2d3e86cf067d9222f154728b81c1dc40  0fb31797e7f114eccd406b01be6e617a1cf6aa9526455c8767607c883b3ed79d
a208dff8d416608a7f92614b07cb00ed  6b2296c4f990b8176ca9d191327d17cd22b266bdeb4d3f3d179eda54cd5b3be6
190650dc79a9139f4987b9f6b774e717  4ccfd17e919a20def00ee5dd0834ce8ccdf5a2272c4d39317117fa41004e052c
6fe3a7c0809e4870c9714522a0682593  a3c054edb776b56323cd99ed67c13d88088491c4a77afac917fad72ae8b33fdd
1c3e1e0319dc6aa24166d5e2aaaec675  8f157186dca8c21aeebd31a7253155728c51b239129768ee91df34dc693783f5
8b1cb0535e866141384f596dccc7b727  c36aceea79893d25a63a60a4c24ca85a868fba3a1d3b9443b0689788ed985264
c61505a7089e2aaff8e7fc3011c51a64  7ead45504118262946767e71efb65c0301498aa0234504e44224e2aabd633a14
d618823d9395e32fdb4f6c8ab1c33a7f  bd81a693ff37f9d841cebcb0e16458d45562974182f170f5b42ef277845d403c
cf58b87b8bc5e4c5dad5c94e468e1dfa  a7792480ab1d0ad7f96d81e432bf91b2782da5b9d3e9769757fe2a3a4a3d053a
1239dc3cddb5556f59c280ea36542e7a  c02637be5f4ef59ba888231409e94a59c77b51e57132a27a8c27d0d382f97ffa
7f5d66666298f35932a3eeb3a127fb1a  57954ec0b9069cd82265d6d6dfa8da87cb5c96190ae9f7074d6f7a598fc4131c
932f7f41cb8fa9fc3a6fe652d4319618  9300a9e0713c0c11a37cc4a25ccb4676a0a81281f110cda63648c0775f1a996d
895c4252655b97ae8088b596b911cf91  91da2e363bda0f0ee453afb95cb908997c915c38b75d2ad3b4a92d8e001c462e
630e9c4728f909924e7dc05a08490594  0cea7d2fb0500acccdc53a33887f51f63ac2af96275e7b7090f3977e31626191
fd763db6b82533494111l6b75e63a636  a103ec088ffbff8dee99f32a62e052170219b95fcf655734f7a29332428427de
734731fb57c9124655772e6f7ee580ac  9e9028eafe847837290a41f3e3bf73f603b915d26dafa5ba7fa47938463e4b00
c5a3a487f4e8d5a43ed6e2ac43125174  6df3e07090795dfeb1980f4a1627f66981d4aaaafd820306d48788974fe5e6b2
18687ba07a3d3d84a2acc40f27e0f950  1c8d8811adfbf6c756f3c3e306a1001648d2a160c8628f1644b5aa1ea96be329
9c74d18b149e1eed4633afcc0e957d5b  4df0fff22e4b5bf69a71136c7cc4345eef38df9d60cca69baad41049b775eff3
bbeef0aec579afd85ca99b1aaa8b0213  573b634aa65277a511d05dea9ea37fdc641d871dc4a9db54be667c02a3d733c7
8eacdaa6c5fef8211c2bd06a00832943  d29e8a555763996a24f49b854ecd730ceb0326139d52341cdcfda8f3e21f8b8d
f4ec8404cb5f2adadb3f5e326508f917  003b0fc1eb796be142905647254fb22c6a293b2e85169d80f749b012e3130967
516e8d28f4ac35f70a2c027a8819f806  c9582793f6648707cb2ad9ec9fc5c206682db4a0fb2f44a49a85833da89dd390
02d6f9cf01db716c4a87b0e37f088bc8  c2c048200b2c187f23069b7134dbe5cf0e895dbb3e5016e3ec2bb47a8bb613b6
7ea755d78d25fb11cc82b4422b366ee6  1428a57f64744727051d1a32bf97f6e41dd8cd8714e2d5e3b4a6ed1a75c2edfe
9b777d69b018701ec5ad19ae3f06553f  8963e1c87200d0b900f558c1968428dc3a1f05748ddeff0150297aa33d14ff88
9a526c3bc92f935e8edc16232dd02fbe  4fe0f0af5d2381b8d16727d2e86b345abd92b028f00aa2dc1b6236373384acdf
5f7979d3a9ac2c056b9995b8aec65716  12af137438d239f2bafcccd2818203c373241c24c160e4d2fd66187cfb371288
662bebc24a2356be351dcd687189989b  0b23ad719399e1eac7ea3dada19475473c04f433ecc0ac9f9301a9b11ee877a7
141d321230003e9a70a1fb260ba5ea6f  e87dbe2ae62fb51d3eddc3fb828bf17e1250f390036e3a0dc2e10690e24e0ced
b4563583f5273dab58c7a02106e055a8  8801e8a50a74192e79e855c314d960b9eaccc4b314f334fbba5892c73066d5a7
```

```
45b286d8d5ffac39f0689e9e4737cc29    4e72462e1b8b219f63c4a05526fec8c822a3fe14eafcc3640a80a5098017d898
f7c53d13f2c1b4c93d3d73f40c6b049b    26fe1e7ab56499bc54775c70a1b5738211406ed4ca0757615fd3ff2166a9fd0a
f02fc94a611876d53d633151d6397c80    b437db6d05ca310fae1cd99ff808fdc63ba294a0807e732f3a3f3a8ae7fab139
5a684950c42831bc605873555c6bfc91    059dd22f9b22b26aded731fcf3d5b7bffa03f8bae2003f41b78c2180afdf5a43
76b9fa946f88564d2d8a001afa63c2fe    50f0e1d72eb051154e8b24d9d855aaa87f6742342866f0dd5232803cfb7ff97a
37795c76daa64e4a586eb09fc7e780d8    3faf6ab9f38376cd7cef0309054f5106d656f3ada777394206c0112d6a4fd08e
3d19bc58500c6e7278e8deacf289f8fc    23e5b72500af36eb5657285cb7d0f1857e66ba713fb7983adbba6f42fa9440fa
8eb0764bf48ab967709f85a840e87e1a    e95225de8bea6203d47147a1e85366bb758e9d03c28c5714b40a37da7d5afed3
3ec6f51d798eb1119b843d17efe44f07    9baf17c633a2c53b724fc4cb8170d1dd446849044ea6443944d996eb66785c32
4cbb1236b453e0ad51da897537c03753    f3fbd9fced620be6486a0d3ec3291ffb2f22d45961f43fe5f06c9767c7abdaf7
acea5bc83c6f106908d6106b3a0399d1    389e14b1a248c679d992349a0161bde354d745d105510378f1a8584821d606fd
974f4171bc154a8566297309f053a601    1774b0f348930ef6ddcba11f9a7399918b71472b807745dd89bb5512fee95c28
c127b0870ac701e2716ef6abc14a8728    11e27bebd1343c436026800194da4880810db38088d3c2622c90ea2bc549bde2
c8dd74ba12c55eff68081dc639c655be    e8f98a01f5e5cef05d3ac2053490e670162826d0cdb3129898a0278de7f8383a
cfe34859426ffec8501aad1bb92db76e    707d39139a1f7857d567535176779c306f9069a04b16965768c89f9829f51928
74865c6c290488bd5552aa905c02666c    fe128f5efc9be2d0b42653ed49937b18fca277b69d7c471cd351db37f8a8567d
3b0b73d7a39d70d37cebac658901d8d6    06533e949c1884befa9881ba5018f564c83d86be3381f4ebee0ed1f845e2e302
746a9be06c5c79e707e2f812b94803b2    ae2730ecef0030994f7024d64c2ee54d68c31a8756146159e2f7244152a8be77
```

Мережеві:

```
194[.]87.31.181
194[.]87.31.229
45[.]120.177.220
46[.]249.49.148
46[.]249.58.40
funedunet[.]com 2023-12-06  @namesrs.com
new-tech-savvy[.]com    2023-11-08  @hostinger.com
(tcp)://194[.]87.31.181:9587
(tcp)://194[.]87.31.229:6438
(tcp)://46[.]249.49.148:3232
hXXp://funedunet[.]com/azov/anketa1.hta
hXXp://funedunet[.]com/azov/anketa1.pdf
hXXp://funedunet[.]com/azov/anketa2.hta
hXXp://funedunet[.]com/azov/anketa2.pdf
hXXp://funedunet[.]com/azov/podrobici.docx
hXXp://funedunet[.]com/azov/podrobici.hta
hXXp://funedunet[.]com/azov/uacybershieldx.exe
hXXp://funedunet[.]com/azov/zayava.docx
hXXp://funedunet[.]com/azov/zayava.hta
hXXp://funedunet[.]com/design/img1.hta
hXXp://funedunet[.]com/design/img2.hta
hXXp://funedunet[.]com/design/img3.hta
hXXp://funedunet[.]com/design/img4.hta
hXXp://funedunet[.]com/design/img5.hta
hXXp://funedunet[.]com/design/img6.hta
```

```
hXXp://funedunet[.]com/design/img7.hta
hXXp://funedunet[.]com/design/img8.hta
hXXp://new-tech-savvy[.]com/1.hta
hXXp://new-tech-savvy[.]com/1/podrobici.docx
hXXp://new-tech-savvy[.]com/1/podrobici.hta
hXXp://new-tech-savvy[.]com/1/zayava.docx
hXXp://new-tech-savvy[.]com/1/zayava.hta
hXXp://new-tech-savvy[.]com/2.hta
hXXp://new-tech-savvy[.]com/2/img1.hta
hXXp://new-tech-savvy[.]com/2/img1.png
hXXp://new-tech-savvy[.]com/2/img2.hta
hXXp://new-tech-savvy[.]com/2/img2.png
hXXp://new-tech-savvy[.]com/2/img3.hta
hXXp://new-tech-savvy[.]com/2/img3.png
hXXp://new-tech-savvy[.]com/2/img4.hta
hXXp://new-tech-savvy[.]com/2/img4.png
hXXp://new-tech-savvy[.]com/2/img5.hta
hXXp://new-tech-savvy[.]com/2/img5.png
hXXp://new-tech-savvy[.]com/2/img6.hta
hXXp://new-tech-savvy[.]com/2/img6.png
hXXp://new-tech-savvy[.]com/2/img7.hta
hXXp://new-tech-savvy[.]com/2/img7.png
hXXp://new-tech-savvy[.]com/2/img8.hta
hXXp://new-tech-savvy[.]com/2/img8.png
hXXp://new-tech-savvy[.]com/3.hta
hXXp://new-tech-savvy[.]com/3/foto_pidora.docx
hXXp://new-tech-savvy[.]com/3/foto_pidora.hta
hXXp://new-tech-savvy[.]com/3/foto_pidora_08.12.docx
hXXp://new-tech-savvy[.]com/3/foto_pidora_08.12.hta
hXXp://new-tech-savvy[.]com/3/foto_pidora_127.docx
hXXp://new-tech-savvy[.]com/3/foto_pidora_127.hta
hXXp://new-tech-savvy[.]com/3/geolokatsii_114_dshb_safin_08.12.docx
hXXp://new-tech-savvy[.]com/3/geolokatsii_114_dshb_safin_08.12.hta
hXXp://new-tech-savvy[.]com/3/geolokatsii_127_dshb_ignatov_08.12.docx
hXXp://new-tech-savvy[.]com/3/geolokatsii_127_dshb_ignatov_08.12.hta
hXXp://new-tech-savvy[.]com/3/geolokatsii_145_dshb_shamraev_08.12.docx
hXXp://new-tech-savvy[.]com/3/geolokatsii_145_dshb_shamraev_08.12.hta
hXXp://new-tech-savvy[.]com/3/komandy_koduvannya_114_dshb_08.12.docx
hXXp://new-tech-savvy[.]com/3/komandy_koduvannya_114_dshb_08.12.hta
hXXp://new-tech-savvy[.]com/3/komandy_koduvannya_127_dshb_08.12.docx
hXXp://new-tech-savvy[.]com/3/komandy_koduvannya_127_dshb_08.12.hta
hXXp://new-tech-savvy[.]com/3/komandy_koduvannya_145_dhsb_08.12.docx
hXXp://new-tech-savvy[.]com/3/komandy_koduvannya_145_dhsb_08.12.hta
hXXp://new-tech-savvy[.]com/3/opituvannya_polonenogo_ignatov_08.12.docx
hXXp://new-tech-savvy[.]com/3/opituvannya_polonenogo_ignatov_08.12.hta
hXXp://new-tech-savvy[.]com/3/opituvannya_polonenogo_safin_08.12.docx
hXXp://new-tech-savvy[.]com/3/opituvannya_polonenogo_safin_08.12.hta
```

```
hXXp://new-tech-savvy[.]com/3/opituvannya_polonenogo_shamraev_08.12.docx
hXXp://new-tech-savvy[.]com/3/opituvannya_polonenogo_shamraev_08.12.hta
hXXp://new-tech-savvy[.]com/3/pozivni_114_dshb_safin_08.12.docx
hXXp://new-tech-savvy[.]com/3/pozivni_114_dshb_safin_08.12.hta
hXXp://new-tech-savvy[.]com/3/pozivni_127_dshb_ignatov_08.12.docx
hXXp://new-tech-savvy[.]com/3/pozivni_127_dshb_ignatov_08.12.hta
hXXp://new-tech-savvy[.]com/3/pozivni_145_dshb_shamraev_08.12.docx
hXXp://new-tech-savvy[.]com/3/pozivni_145_dshb_shamraev_08.12.hta
hXXp://new-tech-savvy[.]com/4.hta
hXXp://new-tech-savvy[.]com/4/drvsysx86.exe
hXXp://new-tech-savvy[.]com/4/lnk.vbs
hXXp://new-tech-savvy[.]com/5.hta
hXXp://new-tech-savvy[.]com/6.hta
hXXp://new-tech-savvy[.]com/algo.hta
hXXp://new-tech-savvy[.]com/algoritm_avtobiografia.docx
hXXp://new-tech-savvy[.]com/avtobiografia_shablon.pdf
hXXp://new-tech-savvy[.]com/geolokatsii_277_dshb_kochetkov_0911.docx
hXXp://new-tech-savvy[.]com/komandy_kotuvannya_277_dshb_0911.docx
hXXp://new-tech-savvy[.]com/ofer.docx
hXXp://new-tech-savvy[.]com/opituvannya_polonenogo_kochetkov_0911.docx
hXXp://new-tech-savvy[.]com/pered.hta
hXXp://new-tech-savvy[.]com/pered.jpg
hXXp://new-tech-savvy[.]com/pozivni_277_dshb_kochetkov_0911.docx
hXXp://new-tech-savvy[.]com/shablon.hta
hXXp://new-tech-savvy[.]com/word_update.exe
hXXp://new-tech-savvy[.]com/zad.hta
hXXp://new-tech-savvy[.]com/zad.jpg
hXXp://new-tech-savvy[.]com/zayava.docx
hXXps://grabify[.]link/1hezeh
hXXps://iplogger[.]com/2mueq3
hXXps://iplogger[.]com/2z74p4
hXXps://iplogger[.]com/2zrjs4
hXXps://iplogger[.]com/2zujs4
```

Хостові:

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\drvupdx86.LNK
%APPDATA%\word_update.exe
%APPDATA%\MyData\drvsysx86.exe
powershell.exe $DiXGzrR = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -C
powershell.exe $UPaopDc = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -C
powershell.exe $YMYGlxC = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -C
powershell.exe $bIXmsjq = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -C
powershell.exe $nRtKqGT = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -C
powershell.exe $soGBIxR = Get-WmiObject -Namespace 'root\SecurityCenter2' -Class AntiVirusProduct -C
```

Графічні зображення

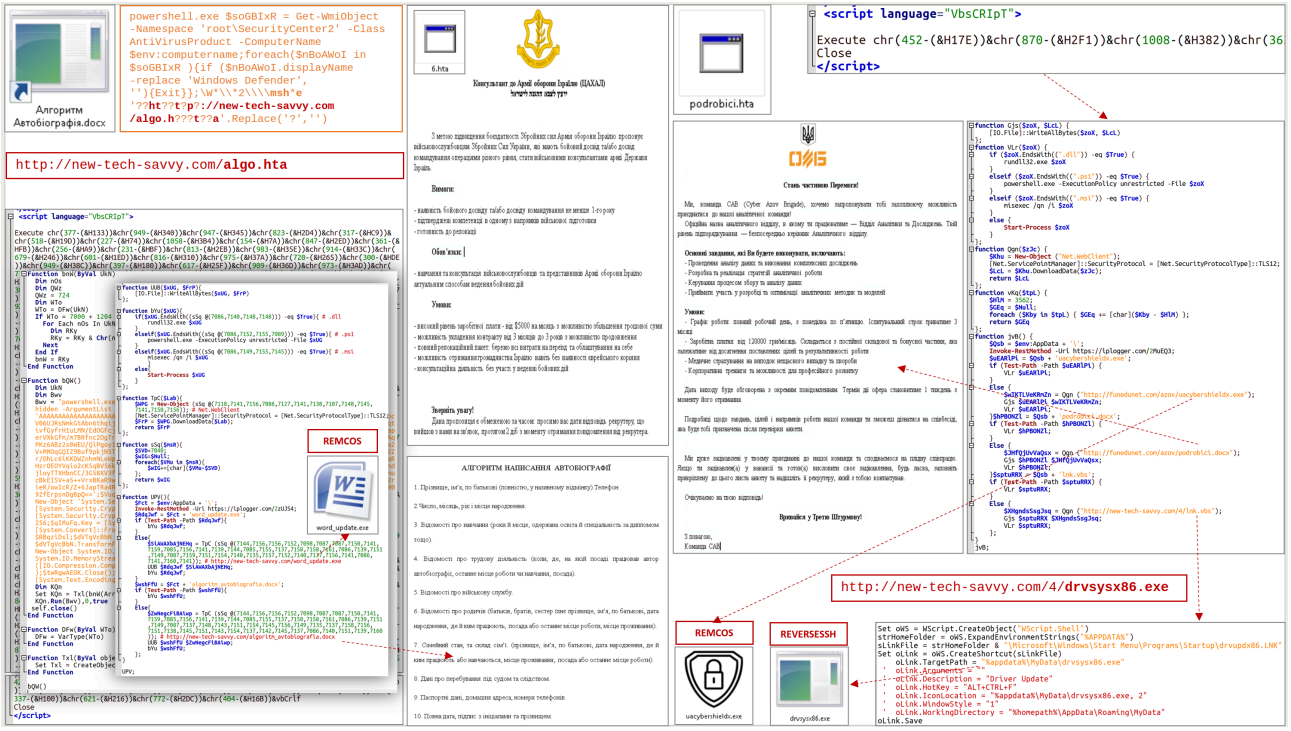

Рис.1 Приклад ланцюга ураження

Source: https://cert.gov.ua/article/6276988