# Файли конфігурацій RDP як засіб отримання віддаленого доступу до комп'ютера або "Rogue RDP" (CERT-UA#11690)

---

**Загальна інформація**

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 22.10.2024 отримано інформацію щодо масового розповсюдження серед органів державної влади, підприємств основних галузей промисловості та військових формувань електронних листів з тематиками, присвяченими, нібито, питанням "інтеграції" з сервісами Amazon, Microsoft та впровадження архітектутри "нульової" довіри (Zero trust architecture, ZTA).

У якості вкладення згадані листи містили конфігураційні файли налаштування протоколу віддаленого робочого столу RDP (".rdp"), запуск яких забезпечував встановлення вихідного RDP-з'єднання з сервером зловмисників. При цьому, зважаючи на параметри RDP-файлу, під час такого RDP-підключення віддаленому серверу не тільки **надавався доступ** до дисків, мережевих ресурсів, принтерів, COM-портів, аудіо-пристроїв, буферу обміну та інших ресурсів на локальному комп'ютері, а й могли бути створені технічні передумови для **запуску на комп'ютері жертви сторонніх програм/скриптів**.

Відповідно до інформації профільних організацій інших країн можемо стверджувати, що активність має широку географію.

Дослідження пов'язаних доменних імен дозволяє припустити, що підготовка інфраструктури для проведення кібератак здійснювалася, щонайменше, з серпня 2024 року. Звертаємо увагу, що IP-адреси та доменні імена, наведені в розділі "Індикатори кіберзагроз", виявлено по ряду схожостей та можуть не мати відношення до розглянутого кіберінциденту.

Очевидно, що скорочення поверхні атаки можна досягнути шляхом комбінації технічних заходів, зокрема:

- блокування ".rdp" файлів на поштовому шлюзі
- блокування можливості запуску будь-яких ".rdp" файлів користувачами (створення виключень)
- налаштування міжмережевого екрану для обмеження можливості встановлення RDP-з'єднань програмою mstsc.exe до ресурсів в мережі Інтернет
- налаштування групових політик (адміністративного шаблону) для заборони перенаправлення ресурсів EOM за допомогою RDP ("Remote Desktop Services" -> "Remote Desktop Session Host" -> "Device and Resource Redirection" -> "***Do not allow...***")

З метою пошуку можливих ознак реалізації описаної кіберзагрози рекомендуємо перевірити журнали мережевої взаємодії з наведеними IP-дресами та доменними іменами, а також, за поточний місяць, окремо проаналізувати легітимність **всіх** вихідних мережевих з'єднань до **будь-яких** IP-адрес в мережі Інтернет (порт 3389/tcp).

Описана активність відстежується за ідентифікатором UAC-0215.

**Індикатори кіберзагроз**

*Файли:*

```
a5de73d69c1a7fbae2e71b98d48fe9b5
34c88cd591f73bc47a1a0fe2a4f594f628be98ad2366eeb4e467595115d8505a    Zero
Trust Architecture Configuration.rdp
8bcb741a204c25232a11a7084aa2221f
071276e907f185d9e341d549b198e60741e2c7f8d64dd2ca2c5d88d50b2c6ffc    ZTS
Device Compatibility Test.rdp
86f58115c891ce91b7364e5ff0314b31
6e6680786fa5b023cf301b6bc5faaa89c86dc34b696f4b078cf22b1b353d5d3c    Device
Configuration Verification.rdp
80b3cad4f70b6ea8924aa13d2730328b
31f2cc1157248aec5135147073e49406d057bebf78b3361dd7cbb6e37708fbcc    Zero
Trust Architecture Configuration.rdp
c0da30b71d58e071fc5863381444d9f0
88fd6a36e8a61597dd71755b985e5fcd0b8308b69fc0f4b0fc7960fb80018622    Device
Security Requirements Check.rdp
1595266bb78dc1e3d67f929154824c74
b8327671ebc20db6f09efc4f19bd8c39d9e28c9a37bdd15b2fd62ade208d2e8a    Device
Security Requirements Check.rdp
222c83d156a41735c38cc552a7084a86
a5bbb109faefcecba695a84a737f5e47fa418cea39d654bb512a6f4a0b148758    Device
Configuration Verification.rdp
fa9af43e9bbb55b7512b369084d91f4d
5534cc837ba4fa3726322883449b3e97ca3e0d28c0ccf468b868397fdfa44e0b    Zero
Trust Architecture Configuration.rdp
281a28800a4ba744bfde7b4aff46f24e
b9ab481e7a9a92cfa2d53de8e7a3c75287cff6a3374f4202ec16ea9e03d80a0b    Zero
Trust Security Environment Compliance Check.rdp
d37cd2c462af0e0643076b20c5ff561e
18a078a976734c9ec562f5dfa3f5904ef5d37000fb8c1f5bd0dc2dee47203bf9    Device
Configuration Verification.rdp
e465a4191a93195094a803e5d4703a90
bb4d5a3f7a40c895882b73e1aca8c71ea40cef6c4f6732bec36e6342f6e2487a    AWS IAM
Quick Start.rdp
3f753810430b26b94a172fbf816e7d76
ef4bd88ec5e8b401594b22632fd05e401658cf78de681f81409eadf93f412ebd    Device
Configuration Verification.rdp
434ffae8cfc3caa370be2e69ffaa95d1
1cfe29f214d1177b66aec2b0d039fec47dd94c751fa95d34bc5da3bbab02213a    Zero
```

Trust Security Environment Compliance Check.rdp
c287c05d91a19796b2649ebebd27394b
3a2496db64507311f5fbd3aba0228b653f673fc2152a267a1386cbab33798db5 ZTS
Device Compatibility Test.rdp
aabbfd1acd3f3a2212e348f2d6f169fc
984082823dc1f122a1bb505700c25b27332f54942496814dfd0c68de0eba59dc AWS IAM
Configuration.rdp
b0a0ad4093e781a278541e4b01daa7a8
383e63f40aecdd508e1790a8b7535e41b06b3f6984bb417218ca96e554b1164b Zero
Trust Security Environment Compliance Check.rdp
a18a1cad9df5b409963601c8e30669e4
296d446cb2ad93255c45a2d4b674bbacb6d1581a94cf6bb5e54df5a742502680 Device
Security Requirements Check.rdp
cbbc4903da831b6f1dc39d0c8d3fc413
129ba064dfd9981575c00419ee9df1c7711679abc974fa4086076ebc3dc964f5 ZTS
Device Compatibility Test.rdp
bd711dc427e17cc724f288cc5c3b0842
f2acb92d0793d066e9414bc9e0369bd3ffa047b40720fe3bd3f2c0875d17a1cb AWS IAM
Quick Start.rdp
b38e7e8bba44bc5619b2689024ad9fca
f357d26265a59e9c356be5a8ddb8d6533d1de222aae969c2ad4dc9c40863bfe8 AWS IAM
Compliance Check.rdp
40f957b756096fa6b80f95334ba92034
280fbf353fdffefc5a0af40c706377142fff718c7b87bc8b0daab10849f388d0 AWS IAM
Configuration.rdp
db326d934e386059cc56c4e61695128e
8b45f5a173e8e18b0d5c544f9221d7a1759847c28e62a25210ad8265f07e96d5 Zero
Trust Security Environment Compliance Check.rdp
f58cf55b944f5942f1d120d95140b800
ba4d58f2c5903776fe47c92a0ec3297cc7b9c8fa16b3bf5f40b46242e7092b46 Zero
Trust Security Environment Compliance Check.rdp

*Мережеві:*

yulia.antonenko@townoflakelure.com
alexandra.gerst@townoflakelure.com
oleksii.myronov@townoflakelure.com

ca-central-1.awsplatform[.]online
ca-west-1.mfa-gov[.]cloud
central-2-aws.ua-aws[.]army
eu-central-1-aws.mfa-gov[.]cloud
eu-central-1.mfa-gov[.]cloud
eu-central-1.ukrtelecom[.]cloud
eu-central-2-aws.ua-aws[.]army

```
eu-north-1-aws.ua-energy[.]cloud
eu-north-1-aws.ua-gov[.]cloud
eu-south-1-aws.mfa-gov[.]cloud
eu-south-2-aws.mfa-gov[.]cloud
eu-southeast-1-aws.gov-ua[.]cloud
eu-southeast-1-aws.govtr[.]cloud
eu-southeast-1-aws.zero-trust[.]solutions
us-east-1-aws.mfa-gov[.]cloud
us-east-2-aws.ua-gov[.]cloud
us-east-console.awsplatform[.]online
us-west-1-amazon.ua-energy[.]cloud
us-west-1.aws-ukraine[.]cloud
us-west-1.ua-aws[.]army
us-west-1.ukrtelecom[.]cloud
us-west-2-aws.mfa-gov[.]cloud

zero-trust.solutions            2024-09-10
ukrtelecom.cloud                    2024-08-15
awsplatform.online                      2024-08-19

aws-ukraine.cloud                       2024-08-15
aws-s3.cloud                            2024-09-16
aws-meet.cloud                          2024-09-20
aws-il.cloud                            2024-09-24
aws-data.cloud                          2024-09-26
aws-meetings.cloud              2024-09-26
aws-secure.cloud                        2024-09-26
aws-join.cloud                          2024-09-27
aws-online.cloud                        2024-10-08

gov-au[.]cloud                          2024-08-07
gov-aws[.]cloud                         2024-09-27
gov-fi[.]cloud                          2024-08-14
gov-gr[.]cloud                          2024-08-14
gov-lt[.]cloud                          2024-08-14
gov-lv[.]cloud                          2024-09-23
gov-pl[.]cloud                          2024-08-23
gov-sk[.]cloud                          2024-08-26
gov-trust[.]cloud                       2024-09-27
gov-ua[.]cloud                          2024-08-15

govps[.]cloud                           2024-08-14
govtr[.]cloud                           2024-08-15
govua[.]cloud                           2024-08-15
```

| | |
|---|---|
| eru-gov[.]cloud | 2024-09-10 |
| feedzai-gov[.]cloud | 2024-10-10 |
| md-gov[.]cloud | 2024-09-10 |
| mf-gov[.]cloud | 2024-09-10 |
| mo-gov[.]cloud | 2024-09-10 |
| mpo-gov[.]cloud | 2024-09-10 |
| mpsv-gov[.]cloud | 2024-09-10 |
| msmt-gov[.]cloud | 2024-09-10 |
| mv-gov[.]cloud | 2024-09-10 |
| my-gov[.]cloud | 2024-08-03 |
| mzd-gov[.]cloud | 2024-09-10 |
| mze-gov[.]cloud | 2024-09-10 |
| mzp-gov[.]cloud | 2024-09-10 |
| mzv-gov[.]cloud | 2024-09-10 |
| nakit-gov[.]cloud | 2024-09-10 |
| nbu-gov[.]cloud | 2024-09-10 |
| nukib-gov[.]cloud | 2024-09-10 |
| policie-gov[.]cloud | 2024-09-10 |
| mmr-gov[.]cloud | 2024-09-10 |
| uohs-gov[.]cloud | 2024-09-10 |
| uoou-gov[.]cloud | 2024-09-10 |
| vlada-gov[.]cloud | 2024-09-10 |
| voa-gov[.]cloud | 2024-09-24 |
| | |
| mfa-gov[.]cloud | 2024-08-15 |
| mfa-gov[.]cloud | 2024-08-15 |
| mfa-gov-il[.]cloud | 2024-09-17 |
| mfa-gov-il[.]cloud | 2024-09-17 |
| mfa-gov-tr[.]cloud | 2024-08-14 |
| mfa-gov-tr[.]cloud | 2024-08-14 |
| | |
| mil-be[.]cloud | 2024-08-21 |
| mil-ee[.]cloud | 2024-08-13 |
| mil-pl[.]cloud | 2024-08-23 |
| mil-pt[.]cloud | 2024-09-09 |
| | |
| mod-gov-il[.]cloud | 2024-09-17 |
| mod-gov-il[.]cloud | 2024-09-17 |
| | |
| s3-acronis[.]cloud | 2024-09-10 |
| s3-army[.]cloud | 2024-08-15 |
| s3-atlassian[.]cloud | 2024-09-09 |
| s3-aws[.]cloud | 2024-09-17 |

s3-bah[.]cloud 2024-09-10
s3-be[.]cloud 2024-08-21
s3-blackberry[.]cloud 2024-09-05
s3-csis[.]cloud 2024-09-12
s3-de[.]cloud 2024-08-26
s3-dgap[.]cloud 2024-09-12
s3-dk[.]cloud 2024-08-21
s3-dnc[.]cloud 2024-09-04
s3-esa[.]cloud 2024-09-03
s3-fbi[.]cloud 2024-09-10
s3-hudson[.]cloud 2024-09-13
s3-ida[.]cloud 2024-09-12
s3-iri[.]cloud 2024-09-12
s3-knowbe4[.]cloud 2024-09-04
s3-marcus[.]cloud 2024-09-13
s3-monitoring[.]cloud 2024-09-09
s3-nato[.]cloud 2024-08-23
s3-ned[.]cloud 2024-09-13
s3-nsa[.]cloud 2024-09-27
s3-proofpoint[.]cloud 2024-09-02
s3-pt[.]cloud 2024-09-04
s3-rackspace[.]cloud 2024-09-03
s3-rand[.]cloud 2024-09-10
s3-spacex[.]cloud 2024-09-13
s3-state[.]cloud 2024-09-12
s3-stig[.]cloud 2024-08-30
s3-ua[.]cloud 2024-08-28
s3-ucia[.]cloud 2024-09-10
s3-zoho[.]cloud 2024-09-17

ua-aws.army 2024-09-12
ua-energy[.]cloud 2024-08-26
ua-gov[.]cloud 2024-08-19
ua-gov[.]cloud 2024-08-19
ua-mil[.]cloud 2024-08-08
ua-sec[.]cloud 2024-08-21
ua-se[.]cloud 2024-10-12
ua-sn[.]cloud 2024-10-12

37.153.155[.]143 (Email)
45.42.142[.]49 (Email)
45.42.142[.]89 (Email)
199.204.86[.]87 (Email)
181.215.148[.]194 (Email)

104.247.120[.]157 (Email)
204.111.198[.]27 (Email)
136.0.0[.]11 (Email)

38.180.110[.]238
179.43.148[.]82
45.11.230[.]105
45.141.58[.]60
95.217.113[.]133
185.187.155[.]74
141.195.117[.]125
185.76.79[.]178
2.58.201[.]112
89.46.234[.]115
84.32.188[.]193
38.180.146[.]210
84.32.188[.]197
45.80.193[.]9
45.67.85[.]40
45.134.111[.]123
84.32.188[.]153
62.72.7[.]213
93.188.163[.]16
23.160.56[.]122
95.156.207[.]121
84.32.188[.]148
166.0.187[.]233
185.216.72[.]196
38.180.146[.]230
84.32.188[.]200
45.11.231[.]8
162.252.175[.]233
13.49.21[.]253
179.43.163[.]18
46.19.141[.]186
193.29.59[.]9
135.181.130[.]232
45.134.110[.]83
185.187.155[.]73
23.160.56[.]100

**Графічні зображення**

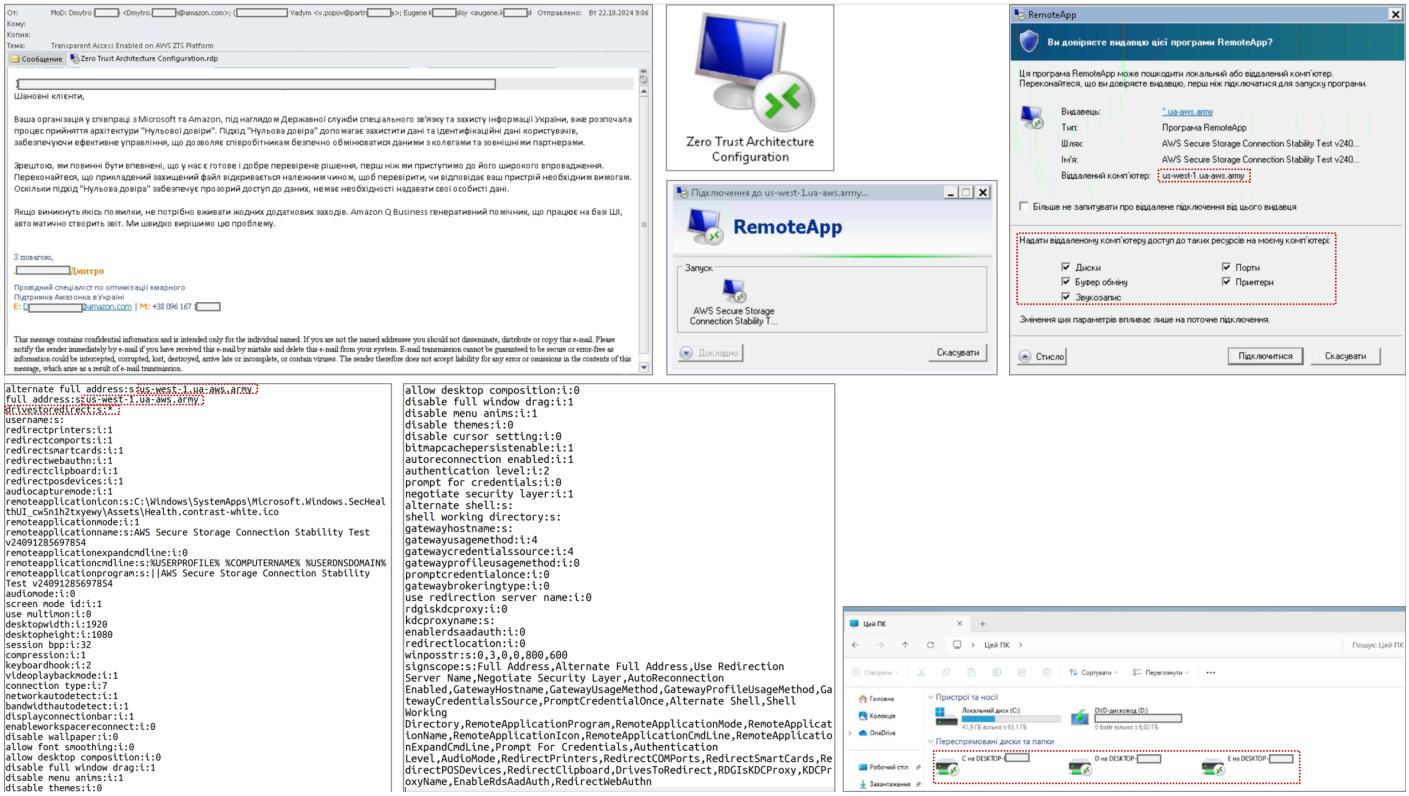


Рис.1 Приклад ланцюга ураження