CERT-UA

Archived: 2026-04-05 23:05:51 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA з 19.07.2022 фіксуються факти масового розсилання електронних листів з темою "Остаточний платіж" та одноіменним вкладенням у вигляді TGZ-архіву.

Архів містить EXE-файл, що класифіковано як .NET-даунлоадер RelicRace, призначений для завантаження (здебільшого з OneDrive), декодування та запуску в пам'яті шкідливої .NET-програми RelicSource.

RelicSource функціонально є інсталятором, що забезпечує дешифрування даних, які зберігаються в ресурсах (можливі варіанти: XOR/DES/DES3/AES/ARC2) та запуск (в т.ч. шляхом інжектування) отриманого пейлоаду. Передбачено декілька способів забезпечення персистентності, імплементовано техніки антианалізу (виявлення VM), а також відправка нотифікацій до Telegram та інше.

Як пейлоад використовуються програми-стілери, а саме: Formbook та Snake Keylogger (ексфільтрація за допомогою API Telegram).

Активність має систематичний, масовий та географічно розосереджений характер і відстежується за ідентифікатором UAC-0041.

Індикатори компрометації

Файли:

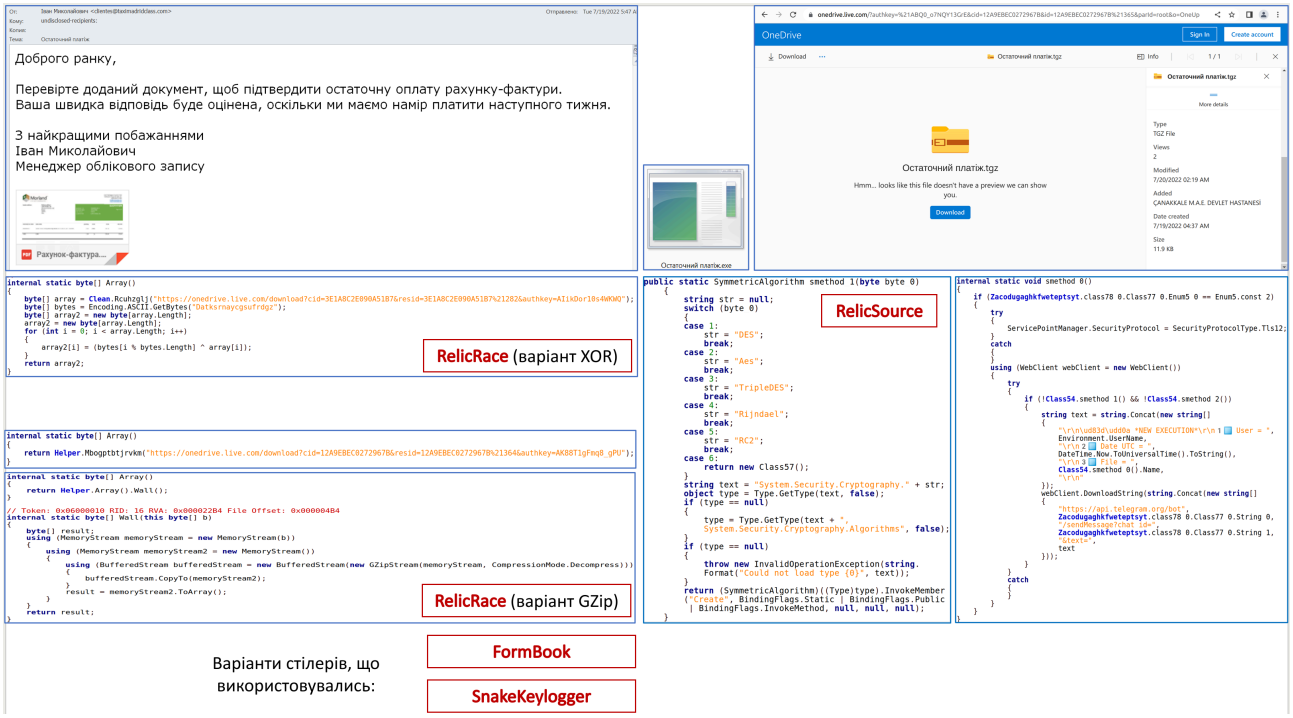
```
538efbb51d22ab4ee22525b17e0e38d8    ca0c1e2011c1229ab3e369079dfb176ff57b64c54e72e900a9e6e32fe0aad1ad
4ab25362247f8a6eb514e80542da4184    1d9aa41d306e5fd6c6ae7d0e6fc518de8d85a45e64a660820023a40234100690
22133c78289867c714dc8d2058003470    39fd4cb19145bc84f60b9ce160a872bae5217396b28819725ed008bbdbd026d0
e21b77a652fa5b52f83ea2bb5adf3e88    60d2f8bc8fd84aae4e0bc4a1c59f95fd6e47d521ec3b9fc78a9eff09e08873da
3f7a9d78d7126c5ebb92b09a7077cf5b    704b0ac0db2351f5fbc213ecb4193f96e37600a5b28992eaf961ea1b9bc39f8f
9e209ae96f1efc0bf7e7df50ae359659    385cf7391e9edbe025702e55e488f6b706cfba3bc60a9158f6bfa8b04456b34a
9ca8df76fca206d90505afc1679ed997    2d3b9f680c4da580ef2e86302e42f4a98965e464b3e3419eb0d17ee8f12f1241
8c7fd60c8dd2ca3ec68684f429e1e5a2    150d21ebf144edea3f56e4a527d2e80458807e0f354d5c9e9b268aded72a2ce0
23d5d360f42203ab62ccdb1cc3a83f79    522833f73d833d6241ea7432376fd8ab4dfc17ed18330a9c5d197faa217d1f0b
d62ae54fff793497fb9068e7349b02f4    ed7cffa33cba2ae44d44f61137d598743a1e9a3c20a66d5a77381e39846ad3be
```

Мережеві:

```
clientes@taximadridclass.com
info@kivanclardokum.com.tr
hXXps://onedrive.live[.]com/download?cid=3E1A8C2E090A51B7&resid=3E1A8C2E090A51B7!282&authkey=AIikDor
```

```
hXXps://onedrive.live[.]com/download?cid=12A9EBEC0272967B&resid=12A9EBEC0272967B!364&authkey=AK88T1g
hXXps://onedrive.live[.]com/download?cid=12A9EBEC0272967B&resid=12A9EBEC0272967B!367&authkey=AB5pQ7L
hXXps://onedrive.live[.]com/download?cid=12A9EBEC0272967B&resid=12A9EBEC0272967B!365&authkey=ABQ0_o7
hXXps://onedrive.live[.]com/download?cid=3E1A8C2E090A51B7&resid=3E1A8C2E090A51B7!283&authkey=AEck4b6
hXXps://onedrive.live[.]com/download?cid=12A9EBEC0272967B&resid=12A9EBEC0272967B!369&authkey=AK3mNiv
hXXps://t[.]co/YLXVIKjfYf
hXXp://barbacoalosmartinez[.]com/pg21/
barbacoalosmartinez[.]com
```

Графічні зображення



Source: https://cert.gov.ua/article/955924