

## Кібератака UAC-0050 у відношенні державних органів України із застосуванням програми для віддаленого контролю та спостереження Remcos (CERT-UA#5926)

---

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA зафіксовано масове розповсюдження електронних листів, начебто, від АТ "Укртелеком", з темою "Судова претензія за Вашим особовим рахунком # 7192206443063763 от: 06.02.2023" та додатком у вигляді RAR-архіву "судовий лист, інформація щодо заборгування.rar".

Архів містить текстовий документ "Ваш персональний код доступу -254507.txt" та ще один RAR-архів "судовий лист, інформація щодо заборгування. pdf.rar", захищений паролем. В другому архіві знаходиться виконуваний файл "судовий лист, інформація щодо заборгування.pdf.exe", розміром більше 600МБ.

Запуск EXE-файлу призведе до встановлення на комп'ютері жертви програми для віддаленого контролю та спостереження Remcos, що є розробкою компанії "BreakingSecurity" (на вебсайті виробника можливо завантажити безкоштовну версію продукту; мінімальна вартість варіанту "Professional" становить 58€).

Виявлена активність відстежується за ідентифікатором UAC-0050, щонайменше, з 2020 року. Попередні кібератаки згаданої групи здійснювалися із застосуванням програми для віддаленого адміністрування RemoteUtilities.

Виходячи з того, що об'єктами кібератак, зазвичай (але не виключно), є органи державної влади України, а також, беручи до уваги функціонал використовуваних програм, вважаємо, що активність здійснюється з метою шпигунства.

### Індикатори компрометації

#### Файли:

5d2bc8cf04bef0aec1dc0fa65fb6ab53

f1103f0e35b7b47f020f951f07a87c74275aaces6a2610690a0f80e34e8eae73

судовий лист, інформація щодо заборгування.rar

8712bdd0adcdab3a6cd7bc5886b6facc

6438fd91958ed9da098e6efd518cbad889f0411cabb7e5a9dd26f810907764e0

Ваш

персональний код доступу -254507.txt

83db7ccad37b6be6cd10d5cd9301a1ea

5047f53e2e496b38b1a11bc856c79d6602fb28f7a0b16a4c4082845dee225677

судовий лист, інформація щодо заборгування. pdf.rar

43a4ce40b5f06ddce984176ae6c89058  
644f8bf83d861db06b736b1d5e541e35d3eae75a74d6f2561fa26a9a271a2c2b  
судовий лист, інформація щодо заборгування.pdf.exe  
ee42511075de43ee5be1f719b9d821f3  
ca408a4f313a8dc8afe42b490e74b345d758bc319c0b5b251f03fed84e8deb0e 2.exe  
(sql.exe) Remcos

### ***Хостові:***

%USERPROFILE%\sql\sql.exe  
%TEMP%\2.exe  
\Sessions\1\BaseNamedObjects\Rgh-LGM500  
HKCU\Software\Rgh-LGM500  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\skype\_upd

### ***Мережеві:***

info@telecomds.online  
gluschko.i.k@ukrtelecom.ua (підроблена адреса)  
telecomds[.]online  
80[.]78.254.28  
101[.]99.91.158  
94[.]131.99.153  
124[.]88.67.67  
124[.]88.67.98  
94[.]131.99.156  
94[.]131.99.89  
94[.]131.99.56  
178[.]23.190.252  
178[.]23.190.253  
178[.]23.190.254  
178[.]23.190.54  
tcp://101[.]99.91.158:5222  
tcp://94[.]131.99.153:8080  
tcp://124[.]88.67.67:5222  
tcp://124[.]88.67.98:5222  
tcp://94[.]131.99.153:5222  
tcp://94[.]131.99.156:5222  
tcp://94[.]131.99.89:5222  
tcp://94[.]131.99.56:5222  
tcp://178[.]23.190.252:8080  
tcp://178[.]23.190.253:8080

tcp://178[.]23.190.254:8080

tcp://178[.]23.190.54:8080

## Графічні зображення

The image shows two screenshots of an email interface. The top screenshot is from 05.02.23, 23:37, with subject 'Судова претензія за Вашим особовим рахунком # 7165868248821980 от: 06.02.2023'. The text states a debt of 9753 UAH and a deadline of 08.02.2023. The bottom screenshot is from 10:31, with subject 'Судова претензія за Вашим особовим рахунком # 7192206443063763 от: 06.02.2023'. The text states a debt of 6069 UAH and the same deadline. Both emails mention a personal access code 254507 and are signed with individual digital signatures.

