CERT-UA

Archived: 2026-04-06 00:07:50 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо здійснення цільових кібератак у відношенні державних службовців, військових, представників оборонних підприємств України з використанням шкідливої програми DarkCrystal RAT, яка розповсюджується засобами месенджеру Signal. При цьому, характерною ознакою є той факт, що відправником може бути людина зі списку контактів і/або спільних груп, що, за задумом, повинно підвищити рівень довіри до таких повідомлень.

Зловмисниками надсилається архів, пароль, а також повідомлення щодо необхідності відкриття файлу **саме на комп'ютері**.

Як правило згаданий архів містить виконуваний файл (розширення: ".pif", ".exe"), який є RARSFX-архівом, в якому, у свою чергу, знаходиться VBE-файл, BAT-файл, та EXE-файл, запуск якого призведе до ураження комп'ютера шкідливою програмою DarkCrystal RAT, що створить технічну можливість прихованого несанкціонованого доступу до ЕОМ.

Вкотре відмічаємо тенденцію до підвищення інтенсивності кібератак з використанням месенджерів та легітимних скомпрометованих облікових записів. При цьому, так чи інакше, жертву спонукають до відкриття файлу на комп’ютері - слід врахувати як окрему пересторогу.

Принагідно наголошуємо на важливості налаштування багато факторної автентифікації https://cert.gov.ua/article/6278274.

У випадку виявлення підозрілих повідомлень, файлів, посилань просимо невідкладно інформувати CERT-UA.

Згадана активність відстежується за ідентифікатором UAC-0200.

Індикатори кіберзагроз

Файли:

```
6903635dc38959f87bbc9aeee3f3555a    d0d6c1f07382ca03866fc3ca198efa8e4a777ecd7ccdc517a4b6ddb7d2d1245e
2e7ef5d68ad7e8df8d621f624127aa14    f26ec43245406c30cc5efb7ad6d8e9018117919c4a03cec2972520e526db3b0c
a64b994390f907703c40d81ec892a5a0    f59e4490a26c421b7d01d05193de927c773b9cbd6cbd91903b422a903ec301a1
6e5a822f6c57d00caaa175b13c05f33d    224e71eea37f1353ea8ee0fef0a513d7f0577dcec3241d6710ad249715a269c7
8b64442e76a6bc0db99e74a95964d3e0    a7f896b2a2433fd178afffba59ace1c27ec4b4fa20ecc59ee7da7c96314c6b09
5a7b9f20b7990c54a716ebcd43960123    1418111224c143fba191efa1fe1a1c4a653b951e4bb07f6fd0b7782631571b93
47aa8d5d45c05c05be3941e43009a5ec    ef6cd2c75b3370d1bcc95beb573ad09861e0ed22b2becc1c16cfff88dae5a157
27e9287a7ac9ca4d8f2ebd7751756594    3ad5473cee7a16bddce171e42b2dbb42caf1bdfbf8f2ef280d956a9940500520
```

```
94124f22d7aa29ab91d40d4f207e1887    8cc204cdd79c811b2d48d878f4cbfcc2e4db88bfaa17bf2c13351e338f8547b3
c917930fd0f91e5c038c8b06719efca4    6bdd44d7b55d47ebd1a00fec6cfda0506efbacbe05022dada9c9dccb5d60909f
52c52b15629514b8527892644e7ea818    b60ac68e278045aadb9ec3196327a90efebf8b48bbe7819c6bf0f5a4678efd62
3bd344b53bd70e1e77f42bf40c22dfb1    02d657729837838d18bbe6b4bae44cab0e6d3a357836d7cd6a9bb7288543facb
```

Мережеві:

```
188[.]245.50.32
hXXp://188[.]245.50.32/VideocentralLocal/PublicdownloadsWp/python4RequestRequest/Javascript8Geovoiddl
```

Хостові:

```
C:\SavesperfCrtMonitor\agentWinintoHostDhcp.exe
C:\SavesperfCrtMonitor\du5a30GGdpnw9V1NAPFxiabLpStvK7yQccZnAiiXNdT4B.bat
C:\WinSavesbrokerdhcpcommon\0WgIlnTNpgbtjiE2xGB5FgwFA.bat
C:\WinSavesbrokerdhcpcommon\bridgeSurrogatewin.exe
```

Графічні зображення

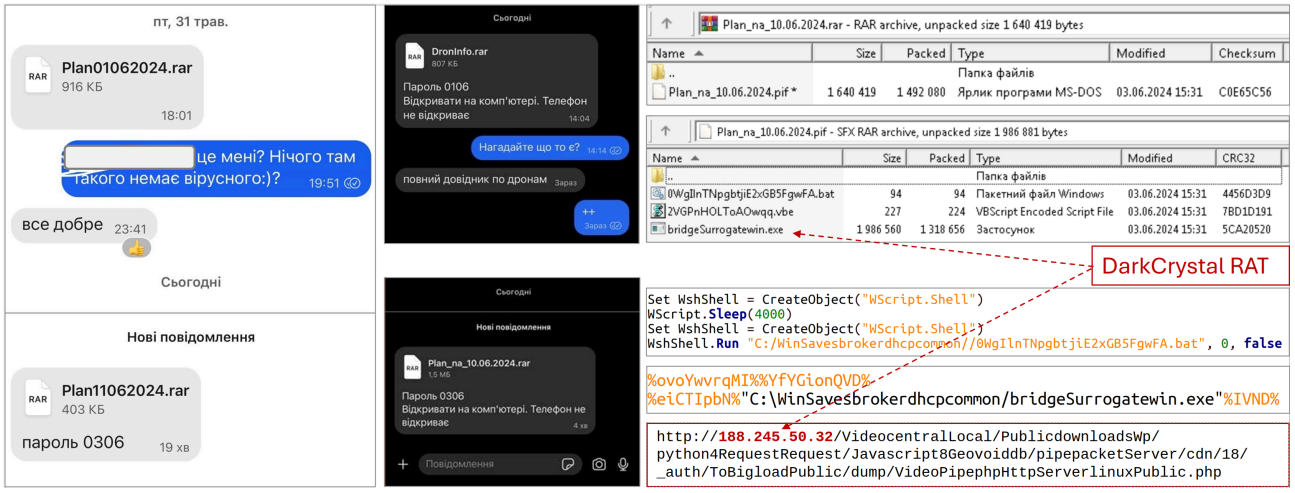

Рис.1 Приклад ланцюга ураження

Source: https://cert.gov.ua/article/6279561