CERT-UA

Archived: 2026-04-05 19:15:25 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено декілька шкідливих файлів зі специфічними назвами: "Вниманию.doc", "17.06.2022_Протокол_МРГ_Подгруппа_ИБ.doc", "замечания таблица 20.06.2022.doc", "О_формировании_проекта_ПНС_2022_файл_отображен.doc".

Згадані RTF-документи містять шкідливий код, що забезпечує експлуатацію однієї або декількох відомих вразливостей в MS Office Word (вірогідно, документи створено за допомогою білдера RoyalRoad). Як результат, комп'ютер жертви буде уражено шкідливою програмою Bisonal (в одному з випадків використовується завантажувач QuickMute).

За даними дослідників кіберзагроз, використання білдеру RoyalRoad є однією з характерних ознак для угруповань, що пов'язують з Китаєм. Більше того, шкідлива програма Bisonal, як приклад, є інструментом групи TontoTeam (UAC-0018).

Зважаючи на викладене, доцільно припустити, що групи, які асоціюють з КНР, активізували діяльність у відношенні російської федерації (підприємства наукового-технічної, авіаційної галузі, а також державні органи).

Рекомендуємо взяти до уваги описаний спосіб здійснення кібератак та ще раз наголошуємо на необхідності вчасного оновлення програмного забезпечення.

Індикатори компрометації

Файли:

```
8cdd56b2b4e1e901f7e728a984221d10    7944fa9cbfef2c7d652f032edc159abeaa1fb4fd64143a8fe3b175095c4519f5
83b8d4462566a23298ca38c418eeccde    f76f3277385195c27fdf2f90a01a8dd70bd05d92ab70696a6e6d7b0d5fb8e70c
2f6d6e783d0c0cbe237714dd34d68e73    7bfb283ee5c283ac6ebae718edb6ed340ab986a095ebab8c13ae828bffbaef9d

80987dcdb36e7cb52bb03f00261aa2bd    c7018ee3783f4b2fb19fedc78c59586390efa1b72c907867794bf42141eb767c
001b53acfab523dc060d38d73d63feef    d79dcb90dfc01723f8df5628f502352c6f922187d3ef5942a6e8465552f40edf
b8387fc571a8e79efab3e2cc343aae24    c2ba362693aad8686f79822712c3871f0da1570465578843f5d73c70db07e631
67bfa75dbc39ab88da995c21565d05ca    7970393e506934e9304f1d18ced34b86ef04a0d278d8e3cdb4b0064caee73846
518439fc23cb0b4d21c7fd39484376ff    0f704f3ab4a3ec30656dab6094c582b1089cbc8fcba280cadf3c7a651aeaacc3
2342bdd79ea84c4fa1b59d224f5a534e    f87b327dd7a3608fec6c0b0bb3486cc8c9b52271fdb3dc0b07229be116ca3786
```

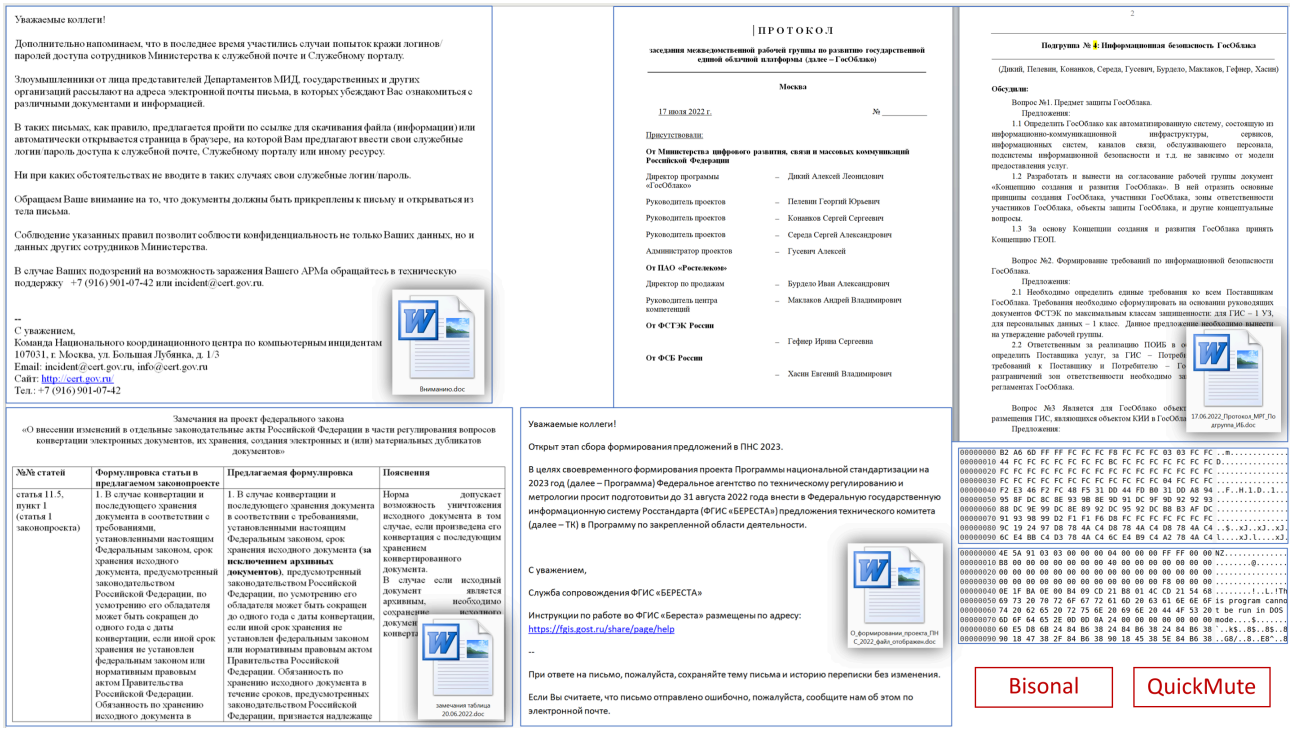
Мережеві:

```
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
hXXps://upportteam.lingrevelat[.]com/update/v32/default
hXXps://upportteam.lingrevelat[.]com
upportteam.lingrevelat[.]com
lingrevelat[.]com
137[.]220.176.165
```

Додаткова інформація

QuickMute - шкідлива програма, розроблена з використанням мови програмування C/C++. Функціонально забезпечує завантаження, RC4-дешифрування та in-memory запуск пейлоаду (очікує PE-файл з експортною функцією "HttpsVictimMain"). Для комунікації з сервером управління передбачено використання ряду протоколів, зокрема: TCP, UDP, HTTP, HTTPS. Разом з тим, в розглянутому зразку імплементовано лише HTTPS (програмний код частини функцій видалено).

Графічні зображення



Source: https://cert.gov.ua/article/375404